(19) (11) Publication number: 2003101527 A

Generated Document.

PATENT ABSTRACTS OF JAPAN

(21) Application number: 2001286881
(22) Application date: 20.09.01
(51) Intl. Cl.: H04L 9/10 G06F 12/14

(30) Priority:
(43) Date of application publication: 04.04.03
(84) Designated contracting states:

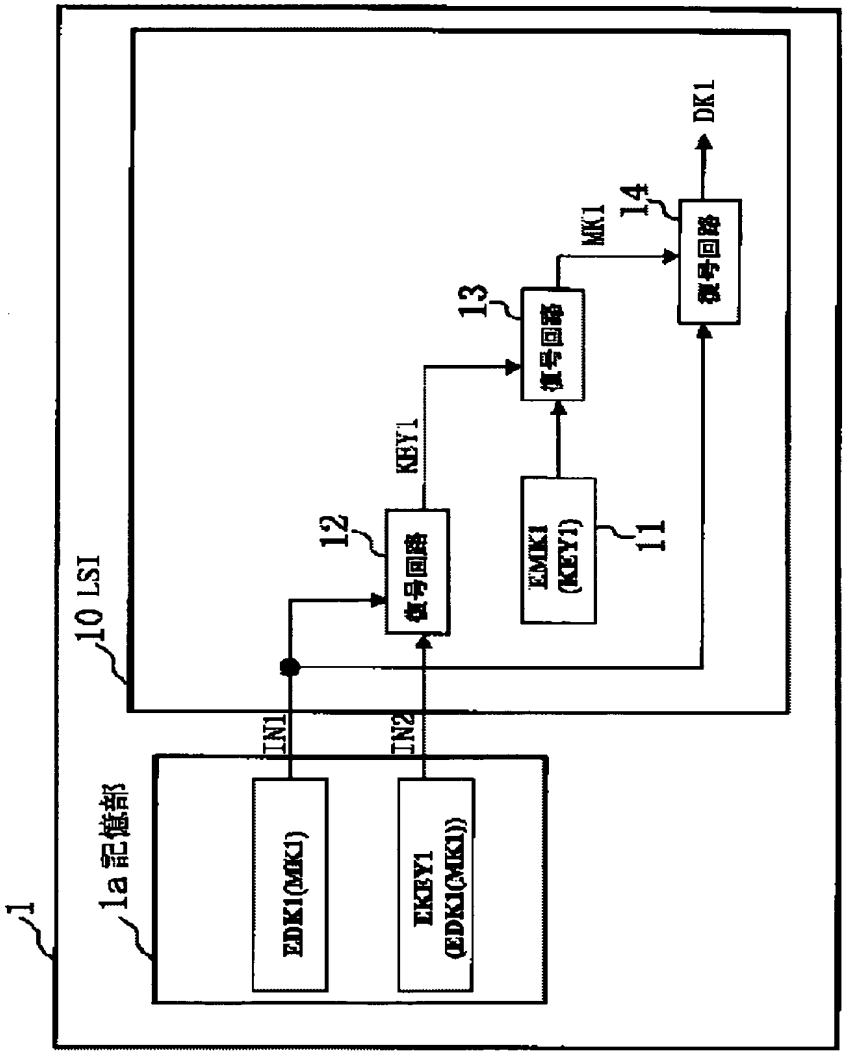
(71) Applicant: MATSUSHITA ELECTRIC IND CO LTD
(72) Inventor: FUJIWARA MUTSUMI
NEMOTO YUSUKE
(74) Representative:

(54) KEY MOUNTING SYSTEM AND LSI FOR IMPLEMENTING THE SAME, AS WELL AS KEY MOUNTING METHOD

(57) Abstract:

PROBLEM TO BE SOLVED: To improve secrecy and concealment for a key in a key mounting system.

SOLUTION: A decryption circuit 12 decrypts an encrypted key EKEY1 (EDK1 (MK1)) using an encrypted key EDK1(MK1) as a key, and a decryption circuit 13 decrypts an encrypted key EMK1 (KEY1) using the output of the decryption circuit 12, namely an internal key KEY1, as a key. A decryption circuit 14 decrypts the encrypted key EDK1(MK1) using the output of the decryption circuit 13, namely an internal key MK1 as a key, and generates a final key DK1. Namely, all of the keys mounted on a storage unit 1a and an LSI 10 are encrypted. Moreover, the final key DK1 is generated at the LSI 10.



(19)日本国特許庁（ＪＰ）　(12)公開特許公報（Ａ）　(11)特許出願公開番号
特開2003－101527
（P2003－101527A）
(43)公開日　平成15年４月４日(2003.4.4)

(51)Int.Cl.⁷	識別記号	ＦＩ		テーマコード（参考）
Ｈ０４Ｌ　9/10		Ｇ０６Ｆ　12/14	３２０Ｂ	５Ｂ０１７
Ｇ０６Ｆ　12/14	３２０	Ｈ０４Ｌ　9/00	６２１Ａ	５Ｊ１０４

審査請求　未請求　請求項の数20　ＯＬ　（全 26 頁）

(21)出願番号　特願2001－286881(P2001－286881)

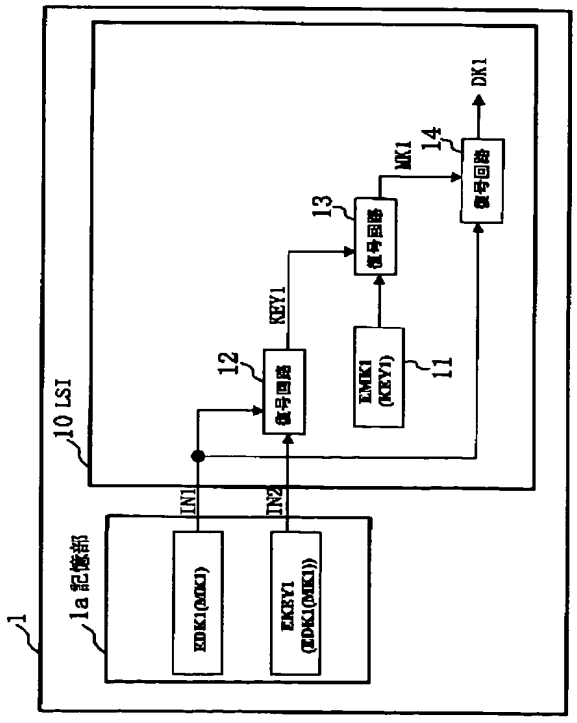
(22)出願日　平成13年９月20日(2001.9.20)

(71)出願人　000005821
松下電器産業株式会社
大阪府門真市大字門真1006番地
(72)発明者　藤原　睦
大阪府門真市大字門真1006番地　松下電器産業株式会社内
(72)発明者　根本　祐輔
大阪府門真市大字門真1006番地　松下電器産業株式会社内
(74)代理人　100077931
弁理士　前田　弘　（外７名）

最終頁に続く

(54)【発明の名称】　鍵実装システムおよびこれを実現するためのＬＳＩ、並びに鍵実装方法

(57)【要約】
【課題】　鍵実装システムにおいて、鍵の機密性および秘匿性をより向上させる。
【解決手段】　復号回路１２は被暗号化鍵ＥＫＥＹ１（ＥＤＫ１（ＭＫ１））を被暗号化鍵ＥＤＫ１（ＭＫ１）を鍵として復号化し、復号回路１３は被暗号化鍵ＥＭＫ１（ＫＥＹ１）を、復号回路１２の出力すなわち内部鍵ＫＥＹ１を鍵として復号化する。復号回路１４は被暗号化鍵ＥＤＫ１（ＭＫ１）を、復号回路１３の出力すなわち内部鍵ＭＫ１を鍵として復号化し、最終鍵ＤＫ１を生成する。すなわち、記憶部１ａおよびＬＳＩ１０に実装された鍵は全て暗号化されたものであり、しかも、ＬＳＩ１０で最終鍵ＤＫ１が生成される。



【特許請求の範囲】
【請求項１】　記憶部と、ＬＳＩとを有する鍵実装システムであって、
前記記憶部は、
最終鍵を、第１の内部鍵を用いて暗号化して得た第１の被暗号化鍵と、
第２の内部鍵を、前記第１の被暗号化鍵を用いて暗号化して得た第２の被暗号化鍵とを記憶しており、
前記ＬＳＩは、
前記第１の内部鍵を、前記第２の内部鍵を用いて暗号化して得た第３の被暗号化鍵を記憶しており、前記記憶部から、前記第１および第２の被暗号化鍵を入力するものであり、かつ、
入力された第２の被暗号化鍵を、入力された第１の被暗号化鍵を鍵として用いて復号化する第１の復号回路と、
前記第３の被暗号化鍵を、前記第１の復号回路の出力を鍵として用いて復号化する第２の復号回路と、
入力された第１の被暗号化鍵を、前記第２の復号回路の出力を鍵として用いて復号化する第３の復号回路とを備えたものであることを特徴とする鍵実装システム。
【請求項２】　請求項１において、前記ＬＳＩは、
第１のテスト用内部鍵を、第２のテスト用内部鍵を用いて暗号化して得た第４の被暗号化鍵をさらに記憶しており、かつ、
前記第３および第４の被暗号化鍵を入力とし、このいずれかを、第１のテスト信号に応じて選択出力する第１のセレクタと、
前記第１のセレクタの選択出力と、前記第２の復号回路の出力とを入力とし、このいずれかを、第２のテスト信号に応じて選択出力する第２のセレクタとを備え、
前記第２の復号回路は、前記第３の被暗号化鍵の代わりに、前記第１のセレクタの出力を入力とするものであり、
前記第３の復号回路は、前記第２の復号回路の出力の代わりに、前記第２のセレクタの出力を鍵として入力するものであることを特徴とする鍵実装システム。
【請求項３】　記憶部と、ＬＳＩとを有する鍵実装システムであって、
前記記憶部は、
最終鍵を、内部鍵を用いて暗号化して得た第１の被暗号化鍵と、
前記内部鍵を、一方向関数による変換によって得た変換鍵を用いて、暗号化して得た第２の被暗号化鍵とを記憶しており、
前記ＬＳＩは、
前記記憶部から、前記第１および第２の被暗号化鍵を入力するものであり、かつ、
前記変換鍵の生成元である変換種を生成する種生成部と、
前記種生成部から出力された変換種を、入力された前記第１の被暗号化鍵を用いて前記一方向関数によって変換し、前記変換鍵を生成する一方向関数回路と、
入力された前記第２の被暗号化鍵を、前記一方向関数回路の出力を鍵として用いて復号化する第１の復号回路と、
入力された前記第１の被暗号化鍵を、前記第１の復号回路の出力を鍵として用いて復号化する第２の復号回路とを備えたものであることを特徴とする鍵実装システム。
【請求項４】　請求項３において、
前記種生成部は、
前記変換種を、記憶するものであることを特徴とする鍵実装システム。
【請求項５】　請求項３において、
前記記憶部は、第１の定数をさらに記憶しており、
前記ＬＳＩは、前記記憶部から、前記第１および第２の被暗号化鍵に加えて、前記第１の定数をさらに入力するものであり、
前記種生成部は、
第２の定数を記憶する定数記憶部と、
前記第２の定数を、入力された前記第１の定数を用いて一方向関数によって変換し、前記変換種を生成する第２の一方向関数回路とを備えたものであることを特徴とする鍵実装システム。
【請求項６】　請求項３において、
前記記憶部は、第１の定数を、前記第１の被暗号化鍵を用いて暗号化して得た第３の被暗号化鍵をさらに記憶しており、
前記ＬＳＩは、前記記憶部から、前記第１および第２の被暗号化鍵に加えて、前記第３の被暗号化鍵をさらに入力するものであり、
前記種生成部は、
入力された前記第３の被暗号化鍵を、入力された前記第１の被暗号化鍵を鍵として用いて復号化する第３の復号回路と、
前記変換種を、前記第１の定数を用いて暗号化して得た第４の被暗号化鍵を記憶する定数記憶部と、
前記第４の被暗号化鍵を、前記第３の復号回路の出力を鍵として用いて復号化し、前記変換種を生成する第４の復号回路とを備えたものであることを特徴とする鍵実装システム。
【請求項７】　請求項３において、
前記記憶部は、
前記内部鍵を、前記一方向関数による変換によって得たテスト用変換鍵を用いて、暗号化して得た第３の被暗号化鍵をさらに記憶しており、
前記ＬＳＩは、
前記記憶部から、前記第１および第２の被暗号化鍵に加えて、前記第３の被暗号化鍵をさらに入力するものであり、かつ、
入力された第２および第３の被暗号化鍵を入力とし、こ

のいずれかを、テスト信号に応じて選択出力する第１のセレクタを備えており、
前記第１の復号回路は、前記第２の被暗号化鍵の代わりに、前記第１のセレクタの出力を入力とするものであり、
前記種生成部は、前記変換種および、前記テスト用変換鍵の生成元であるテスト用変換種のいずれかを、前記テスト信号に応じて選択出力可能に構成されていることを特徴とする鍵実装システム。
【請求項８】　請求項７において、
前記種生成部は、
前記変換種と、前記テスト用変換種とを記憶する定数記憶部と、
前記変換種およびテスト用変換種を入力とし、そのいずれかを、前記テスト信号に応じて選択出力する第２のセレクタとを備えたものであることを特徴とする鍵実装システム。
【請求項９】　請求項７において、
前記種生成部は、
前記変換種の元になる第１の定数と、前記テスト用変換種の元になる第２の定数とを記憶する第１の定数記憶部と、
前記第１および第２の定数を入力とし、そのいずれかを、前記テスト信号に応じて選択出力する第２のセレクタと、
第３の定数を記憶する第２の定数記憶部と、
前記第３の定数を、前記第２のセレクタの出力を用いて、一方向関数によって変換する第２の一方向関数回路とを備えたものであることを特徴とする鍵実装システム。
【請求項１０】　請求項７において、
前記種生成部は、
前記変換種の元になる第１の定数を、前記第１の被暗号化鍵を用いて暗号化して得た第４の被暗号化鍵と、前記テスト用変換鍵の元になる第２の定数を、前記第１の被暗号化鍵を用いて暗号化して得た第５の被暗号化鍵とを記憶する第１の定数記憶部と、
前記第４および第５の被暗号化鍵を入力とし、そのいずれかを、前記テスト信号に応じて選択出力する第２のセレクタと、
前記第２のセレクタの出力を、当該ＬＳＩに入力された前記第１の被暗号化鍵を鍵として用いて復号化する第３の復号回路と、
第３の定数を記憶する第２の定数記憶部と、
前記第３の定数を、前記第３の復号回路の出力を用いて、一方向関数によって変換する第２の一方向関数回路とを備えたものであることを特徴とする鍵実装システム。
【請求項１１】　請求項８～１０のいずれか１項において、
前記ＬＳＩは、
前記第２のセレクタの出力を検証する検証回路を備えたものであることを特徴とする鍵実装システム。
【請求項１２】　請求項３において、
前記ＬＳＩは、
任意の定数が実装可能なヒューズ回路と、
前記第２の復号回路の出力を、前記ヒューズ回路に実装された定数を用いて暗号化し、第３の被暗号化鍵として前記記憶部に出力する暗号回路と、
前記記憶部から入力された第３の被暗号化鍵を、前記ヒューズ回路に実装された定数を用いて復号する第３の復号回路とを備えたものであり、
前記記憶部は、
前記ＬＳＩから前記第３の被暗号化鍵を受けたとき、前記第１および第２の被暗号化鍵を消去してこの第３の被暗号化鍵を記憶するとともに、前記ＬＳＩに前記第３の被暗号化鍵を出力するものであることを特徴とする鍵実装システム。
【請求項１３】　請求項３において、
前記ＬＳＩは、
任意の定数が実装可能なヒューズ回路と、
前記ヒューズ回路に実装された定数を、前記種生成部から出力された変換種を用いて、一方向関数によって変換する第２の一方向関数回路と、
前記第２の復号回路の出力を、前記第２の一方向関数回路の出力を用いて暗号化し、第３の被暗号化鍵として前記記憶部に出力する暗号回路と、
前記記憶部から入力された第３の被暗号化鍵を、前記第２の一方向関数回路の出力を用いて復号化する第３の復号回路とを備えたものであり、
前記記憶部は、
前記ＬＳＩから前記第３の被暗号化鍵を受けたとき、前記第１および第２の被暗号化鍵を消去して、この第３の被暗号化鍵を記憶するとともに、前記ＬＳＩに前記第３の被暗号化鍵を出力することを特徴とする鍵実装システム。
【請求項１４】　請求項１３において、
前記ＬＳＩは、
前記記憶部から入力された第３の被暗号化鍵と、前記暗号回路の出力とを入力とし、このいずれかをテスト信号に応じて選択出力するセレクタを備え、
前記第３の復号回路は、前記記憶部から入力された第３の被暗号化鍵の代わりに、前記セレクタの出力を入力とするものであることを特徴とする鍵実装システム。
【請求項１５】　鍵実装システムを実現するためのＬＳＩであって、
最終鍵を、第１の内部鍵を用いて暗号化して得た第１の被暗号化鍵を第１の入力とし、第２の内部鍵を、前記第１の被暗号化鍵を用いて暗号化して得た第２の被暗号化鍵を第２の入力としたとき、前記最終鍵を生成可能に構

成されており、
前記第１の内部鍵を、前記第２の内部鍵を用いて暗号化して得た第３の被暗号化鍵を記憶する記憶部と、
前記第２の入力を、前記第１の入力を鍵として用いて復号化する第１の復号回路と、
前記第３の被暗号化鍵を、前記第１の復号回路の出力を鍵として用いて復号化する第２の復号回路と、
前記第１の入力を、前記第２の復号回路の出力を鍵として用いて復号化する第３の復号回路とを備えたものであることを特徴とするＬＳＩ。
【請求項１６】　鍵実装システムを実現するためのＬＳＩであって、
最終鍵を、内部鍵を用いて暗号化して得た第１の被暗号化鍵を第１の入力とし、前記内部鍵を、一方向関数による変換によって得た変換鍵を用いて、暗号化して得た第２の被暗号化鍵を、第２の入力としたとき、前記最終鍵をを生成可能に構成されており、
前記変換鍵の生成元である変換種を生成する種生成部と、
前記種生成部から出力された変換種を、前記第１の入力を用いて前記一方向関数によって変換し、前記変換鍵を生成する一方向関数回路と、
前記第２の入力を、前記一方向関数回路の出力を鍵として用いて復号化する第１の復号回路と、
前記第１の入力を、前記第１の復号回路の出力を鍵として用いて復号化する第２の復号回路とを備えたものであることを特徴とするＬＳＩ。
【請求項１７】　請求項１６において、
任意の定数が実装可能なヒューズ回路と、
前記第２の復号回路の出力を、前記ヒューズ回路に実装された定数を用いて暗号化し、第３の被暗号化鍵として当該ＬＳＩ外部に出力する暗号回路と、
当該ＬＳＩの第３の入力を、前記ヒューズ回路に実装された定数を用いて復号する第３の復号回路とを備えたことを特徴とするＬＳＩ。
【請求項１８】　請求項１６において、
任意の定数が実装可能なヒューズ回路と、
前記ヒューズ回路に実装された定数を、前記種生成部から出力された変換種を用いて、一方向関数によって変換する第２の一方向関数回路と、
前記第２の復号回路の出力を、前記第２の一方向関数回路の出力を用いて暗号化し、第３の被暗号化鍵として当該ＬＳＩ外部に出力する暗号回路と、
第３の入力を、前記第２の一方向関数回路の出力を用いて復号化する第３の復号回路とを備えたことを特徴とするＬＳＩ。
【請求項１９】　システムに、鍵を実装する方法であって、
前記システムが有する記憶部に、最終鍵を、第１の内部鍵を用いて暗号化して得た第１の被暗号化鍵と、第２の内部鍵を、前記第１の被暗号化鍵を用いて暗号化して得た第２の被暗号化鍵とを記憶させる工程と、
前記システムに、ＬＳＩを実装する工程とを備え、
前記ＬＳＩは、
前記第１の内部鍵を、前記第２の内部鍵を用いて暗号化して得た第３の被暗号化鍵を記憶しており、前記記憶部から、前記第１および第２の被暗号化鍵を入力するものであり、かつ、
入力された第２の被暗号化鍵を、入力された第１の被暗号化鍵を鍵として用いて復号化する第１の復号回路と、
前記第３の被暗号化鍵を、前記第１の復号回路の出力を鍵として用いて復号化する第２の復号回路と、
入力された第１の被暗号化鍵を、前記第２の復号回路の出力を鍵として用いて復号化する第３の復号回路とを備えたものであることを特徴とする鍵実装方法。
【請求項２０】　システムに、鍵を実装する方法であって、
前記システムが有する記憶部に、最終鍵を、内部鍵を用いて暗号化して得た第１の被暗号化鍵と、前記内部鍵を、一方向関数による変換によって得た変換鍵を用いて暗号化して得た第２の被暗号化鍵とを記憶させる工程と、
前記システムに、ＬＳＩを実装する工程とを備え、
前記ＬＳＩは、
前記記憶部から、前記第１および第２の被暗号化鍵を入力するものであり、かつ、
前記変換鍵の生成元である変換種を生成する種生成部と、
前記種生成部から出力された変換種を、入力された前記第１の被暗号化鍵を用いて前記一方向関数によって変換し、前記変換鍵を生成する一方向関数回路と、入力された前記第２の被暗号化鍵を、前記一方向関数回路の出力を鍵として用いて復号化する第１の復号回路と、
入力された前記第１の被暗号化鍵を、前記第１の復号回路の出力を鍵として用いて復号化する第２の復号回路とを備えたものであることを特徴とする鍵実装方法。
【発明の詳細な説明】
【０００１】
【発明の属する技術分野】本発明は、鍵が実装されたシステムやこれに用いるＬＳＩに関する技術に属する。
【０００２】
【従来の技術】従来の鍵実装システムでは、通常、値が固定された生の鍵を、ＬＳＩ内に実装していた。
【０００３】
【発明が解決しようとする課題】通常のＣＭＯＳＬＳＩの内部では、ＬＳＩの個体毎に違う鍵を実装するのは困難である。すなわち、ＬＳＩ内部に閉じた鍵を変更する手段がない。また、外部ＲＯＭ等からのロードでは、システム（セット）上で解析が可能となる。また、鍵管理者以外に、ＬＳＩ設計者またはシステム（セット）設計

者等が鍵を知るおそれがある。また、違った値の鍵を大量生産技術によって書き込みにくい。また、鍵実装が正確に行われたか否かを検証することができない。すなわち、内部鍵のテストが困難である。

【０００４】前記の問題に鑑み、本発明は、鍵実装システムとして、鍵の機密性および秘匿性をより向上させることを課題とする。

【０００５】また、本発明は、様々な機密鍵を容易に実装することが可能なＬＳＩを提供することを課題とする。

【０００６】さらに、本発明は、鍵実装システムとして、回路規模を増大させることなく、実装された値のテストを可能にすることを課題とする。

【０００７】

【課題を解決するための手段】前記の課題を解決するために、請求項１の発明が講じた解決手段は、記憶部とＬＳＩとを有する鍵実装システムであって、前記記憶部は、最終鍵を第１の内部鍵を用いて暗号化して得た第１の被暗号化鍵と、第２の内部鍵を前記第１の被暗号化鍵を用いて暗号化して得た第２の被暗号化鍵とを記憶しており、前記ＬＳＩは、前記第１の内部鍵を前記第２の内部鍵を用いて暗号化して得た第３の被暗号化鍵を記憶しており、前記記憶部から前記第１および第２の被暗号化鍵を入力するものであり、かつ、入力された第２の被暗号化鍵を入力された第１の被暗号化鍵を鍵として用いて復号化する第１の復号回路と、前記第３の被暗号化鍵を前記第１の復号回路の出力を鍵として用いて復号化する第２の復号回路と、入力された第１の被暗号化鍵を前記第２の復号回路の出力を鍵として用いて復号化する第３の復号回路とを備えたものである。

【０００８】請求項１の発明によると、ＬＳＩにおいて、第１の復号回路によって、記憶部に記憶された第２の被暗号化鍵が、記憶部に記憶された第１の被暗号化鍵を鍵として復号化されて第２の内部鍵が生成され、第２の復号回路によって、ＬＳＩに記憶された第３の被暗号化鍵が、第１の復号回路の出力すなわち第２の内部鍵を鍵として復号化されて第１の内部鍵が生成される。さらに、第３の復号回路によって、第１の被暗号化鍵が、第２の復号回路の出力すなわち第１の内部鍵を鍵として復号化されて最終鍵が生成される。すなわち、記憶部およびＬＳＩに実装された鍵は、全て、暗号化されたものであり、しかも、ＬＳＩで最終鍵が生成される。このため、システム上において、鍵の解析が困難になり、機密性が向上する。また、生の機密鍵を開発者や実装者に与えなくても、ＬＳＩおよびシステムの開発および実装が可能になる。

【０００９】請求項２の発明では、前記請求項１の鍵実装システムにおけるＬＳＩは、第１のテスト用内部鍵を第２のテスト用内部鍵を用いて暗号化して得た第４の被暗号化鍵をさらに記憶しており、かつ、前記第３および第４の被暗号化鍵を入力とし、このいずれかを第１のテスト信号に応じて選択出力する第１のセレクタと、前記第１のセレクタの選択出力と前記第２の復号回路の出力とを入力とし、このいずれかを第２のテスト信号に応じて選択出力する第２のセレクタとを備えたものとし、前記第２の復号回路は、前記第３の被暗号化鍵の代わりに前記第１のセレクタの出力を入力とするものとし、前記第３の復号回路は、前記第２の復号回路の出力の代わりに前記第２のセレクタの出力を鍵として入力するものとする。

【００１０】請求項２の発明によると、まず、第１のセレクタは第４の被暗号化鍵を選択し、第２のセレクタは第２の復号回路の出力を選択するよう、第１および第２のテスト信号を設定する。このとき、第１の復号回路に、テスト用最終鍵を第１のテスト用内部鍵を鍵として用いて暗号化して得た開発用被暗号化鍵を、鍵として与えるとともに、この開発用被暗号化鍵を鍵として用いて第２のテスト用内部鍵を暗号化して得た被暗号化鍵を、復号化の対象として与える。これにより、第１の復号回路から第２のテスト用内部鍵が生成され、第２の復号回路から第１のテスト用内部鍵が生成される。そして、第３の復号回路に、前記開発用被暗号化鍵を復号化の対象として与えることによって、テスト用最終鍵が生成される。すなわち、実際の最終鍵を生成することなく、第１～第３の復号回路が正常に動作するか否かをテストすることができる。

【００１１】また、第１のセレクタは第３の被暗号化鍵を選択し、第２のセレクタは第１のセレクタの出力すなわち第３の被暗号化鍵を選択するよう、第１および第２のテスト信号を設定する。このとき、第３の復号回路に、第３の被暗号化鍵を鍵として用いてテスト用最終鍵を暗号化して得た被暗号化鍵を、復号化の対象として与える。この被暗号化鍵は第３の復号回路によって、第３の被暗号化鍵を鍵として復号化され、これにより、テスト用最終鍵が生成される。すなわち、実際の最終鍵を生成することなく、第３の被暗号化鍵が正しく実装されているか否かをテストすることができる。

【００１２】また、請求項３の発明が講じた解決手段は、記憶部とＬＳＩとを有する鍵実装システムとして、前記記憶部は、最終鍵を内部鍵を用いて暗号化して得た第１の被暗号化鍵と、前記内部鍵を一方向関数による変換によって得た変換鍵を用いて暗号化して得た第２の被暗号化鍵とを記憶しており、前記ＬＳＩは、前記記憶部から、前記第１および第２の被暗号化鍵を入力するものであり、かつ、前記変換鍵の生成元である変換種を生成する種生成部と、前記種生成部から出力された変換種を入力された前記第１の被暗号化鍵を用いて前記一方向関数によって変換し、前記変換鍵を生成する一方向関数回路と、入力された前記第２の被暗号化鍵を前記一方向関数回路の出力を鍵として用いて復号化する第１の復号回

路と、入力された前記第１の被暗号化鍵を前記第１の復号回路の出力を鍵として用いて復号化する第２の復号回路とを備えたものである。

【００１３】請求項３の発明によると、ＬＳＩにおいて、一方向関数回路によって、種生成部から生成された変換種は第１の被暗号化鍵を用いて変換され、変換鍵が生成される。そして第１の復号回路によって、第２の被暗号化鍵が変換鍵を鍵として用いて復号化されて内部鍵が生成され、第２の復号回路によって、第１の被暗号化鍵が内部鍵を鍵として復号されて最終鍵が生成される。ここで、内部鍵を異なる値に変更するとき、第１の被暗号化鍵を新たに生成し、同一の変換種を用いて一方向関数によって新たな変換鍵を生成し、さらに第２の被暗号化鍵を新たに生成すればよい。すなわち、変換種を変えることなく、内部鍵や第１および第２の被暗号化鍵を任意に設定することができるので、共通のＬＳＩを用いて、システム毎に個別に、暗号化する鍵を設定することができる。

【００１４】そして、請求項４の発明では、前記請求項３の鍵実装システムにおける種生成部は、前記変換種を記憶するものとする。

【００１５】また、請求項５の発明では、前記請求項３の鍵実装システムにおいて、前記記憶部は第１の定数をさらに記憶しており、前記ＬＳＩは、前記記憶部から、前記第１および第２の被暗号化鍵に加えて前記第１の定数をさらに入力するものであり、前記種生成部は、第２の定数を記憶する定数記憶部と、前記第２の定数を入力された前記第１の定数を用いて一方向関数によって変換し、前記変換種を生成する第２の一方向関数回路とを備えたものとする。

【００１６】また、請求項６の発明では、前記請求項３の鍵実装システムにおいて、前記記憶部は、第１の定数を前記第１の被暗号化鍵を用いて暗号化して得た第３の被暗号化鍵をさらに記憶しており、前記ＬＳＩは、前記記憶部から、前記第１および第２の被暗号化鍵に加えて前記第３の被暗号化鍵をさらに入力するものであり、前記種生成部は、入力された前記第３の被暗号化鍵を入力された前記第１の被暗号化鍵を鍵として用いて復号化する第３の復号回路と、前記変換種を前記第１の定数を用いて暗号化して得た第４の被暗号化鍵を記憶する定数記憶部と、前記第４の被暗号化鍵を前記第３の復号回路の出力を鍵として用いて復号化し、前記変換種を生成する第４の復号回路とを備えたものとする。

【００１７】また、請求項７の発明では、前記請求項３の鍵実装システムにおいて、前記記憶部は、前記内部鍵を、前記一方向関数による変換によって得たテスト用変換鍵を用いて暗号化して得た第３の被暗号化鍵をさらに記憶しており、前記ＬＳＩは、前記記憶部から、前記第１および第２の被暗号化鍵に加えて前記第３の被暗号化鍵をさらに入力するものであり、かつ、入力された第２および第３の被暗号化鍵を入力とし、このいずれかをテスト信号に応じて選択出力する第１のセレクタを備えており、前記第１の復号回路は、前記第２の被暗号化鍵の代わりに前記第１のセレクタの出力を入力とするものであり、前記種生成部は、前記変換種および、前記テスト用変換鍵の生成元であるテスト用変換種のいずれかを、前記テスト信号に応じて選択出力可能に構成されているものとする。

【００１８】そして、請求項８の発明では、前記請求項７の鍵実装システムにおける種生成部は、前記変換種と前記テスト用変換種とを記憶する定数記憶部と、前記変換種およびテスト用変換種を入力とし、そのいずれかを前記テスト信号に応じて選択出力する第２のセレクタとを備えたものとする。

【００１９】また、請求項９の発明では、前記請求項７の鍵実装システムにおける種生成部は、前記変換種の元になる第１の定数と前記テスト用変換種の元になる第２の定数とを記憶する第１の定数記憶部と、前記第１および第２の定数を入力とし、そのいずれかを前記テスト信号に応じて選択出力する第２のセレクタと、第３の定数を記憶する第２の定数記憶部と、前記第３の定数を、前記第２のセレクタの出力を用いて一方向関数によって変換する第２の一方向関数回路とを備えたものとする。

【００２０】また、請求項１０の発明では、前記請求項７の鍵実装システムにおける種生成部は、前記変換種の元になる第１の定数を前記第１の被暗号化鍵を用いて暗号化して得た第４の被暗号化鍵と、前記テスト用変換鍵の元になる第２の定数を前記第１の被暗号化鍵を用いて暗号化して得た第５の被暗号化鍵とを記憶する第１の定数記憶部と、前記第４および第５の被暗号化鍵を入力とし、そのいずれかを前記テスト信号に応じて選択出力する第２のセレクタと、前記第２のセレクタの出力を当該ＬＳＩに入力された前記第１の被暗号化鍵を鍵として用いて復号化する第３の復号回路と、第３の定数を記憶する第２の定数記憶部と、前記第３の定数を、前記第３の復号回路の出力を用いて一方向関数によって変換する第２の一方向関数回路とを備えたものとする。

【００２１】そして、請求項１１の発明では、前記請求項８～１０のいずれか１項におけるＬＳＩは、前記第２のセレクタの出力を検証する検証回路を備えたものとする。

【００２２】また、請求項１２の発明では、前記請求項３の鍵実装システムにおいて、前記ＬＳＩは、任意の定数が実装可能なヒューズ回路と、前記第２の復号回路の出力を前記ヒューズ回路に実装された定数を用いて暗号化し、第３の被暗号化鍵として前記記憶部に出力する暗号回路と、前記記憶部から入力された第３の被暗号化鍵を前記ヒューズ回路に実装された定数を用いて復号する第３の復号回路とを備えたものとし、前記記憶部は、前記ＬＳＩから前記第３の被暗号化鍵を受けたとき、前記

第１および第２の被暗号化鍵を消去してこの第３の被暗号化鍵を記憶するともに前記ＬＳＩに前記第３の被暗号化鍵を出力するものとする。

【００２３】また、請求項１３の発明では、前記請求項３の鍵実装システムにおいて、前記ＬＳＩは、任意の定数が実装可能なヒューズ回路と、前記ヒューズ回路に実装された定数を、前記種生成部から出力された変換種を用いて一方向関数によって変換する第２の一方向関数回路と、前記第２の復号回路の出力を前記第２の一方向関数回路の出力を用いて暗号化し、第３の被暗号化鍵として前記記憶部に出力する暗号回路と、前記記憶部から入力された第３の被暗号化鍵を前記第２の一方向関数回路の出力を用いて復号化する第３の復号回路とを備えたものとし、前記記憶部は、前記ＬＳＩから前記第３の被暗号化鍵を受けたとき、前記第１および第２の被暗号化鍵を消去してこの第３の被暗号化鍵を記憶するともに、前記ＬＳＩに前記第３の被暗号化鍵を出力するものとする。

【００２４】そして、請求項１４の発明では、前記請求項１３の鍵実装システムにおいて、前記ＬＳＩは、前記記憶部から入力された第３の被暗号化鍵と前記暗号回路の出力とを入力とし、このいずれかをテスト信号に応じて選択出力するセレクタを備え、前記第３の復号回路は、前記記憶部から入力された第３の被暗号化鍵の代わりに前記セレクタの出力を入力とするものとする。

【００２５】また、請求項１５の発明が講じた解決手段は、鍵実装システムを実現するためのＬＳＩとして、最終鍵を第１の内部鍵を用いて暗号化して得た第１の被暗号化鍵を第１の入力とし、第２の内部鍵を前記第１の被暗号化鍵を用いて暗号化して得た第２の被暗号化鍵を第２の入力としたとき、前記最終鍵を生成可能に構成されており、前記第１の内部鍵を前記第２の内部鍵を用いて暗号化して得た第３の被暗号化鍵を記憶する記憶部と、前記第２の入力を前記第１の入力を鍵として用いて復号化する第１の復号回路と、前記第３の被暗号化鍵を前記第１の復号回路の出力を鍵として用いて復号化する第２の復号回路と、前記第１の入力を前記第２の復号回路の出力を鍵として用いて復号化する第３の復号回路とを備えたものである。

【００２６】また、請求項１６の発明が講じた解決手段は、鍵実装システムを実現するためのＬＳＩとして、最終鍵を内部鍵を用いて暗号化して得た第１の被暗号化鍵を第１の入力とし、前記内部鍵を一方向関数による変換によって得た変換鍵を用いて暗号化して得た第２の被暗号化鍵を第２の入力としたとき、前記最終鍵をを生成可能に構成されており、前記変換鍵の生成元である変換種を生成する種生成部と、前記種生成部から出力された変換種を前記第１の入力を用いて前記一方向関数によって変換し、前記変換鍵を生成する一方向関数回路と、前記第２の入力を前記一方向関数回路の出力を鍵として用いて復号化する第１の復号回路と、前記第１の入力を前記第１の復号回路の出力を鍵として用いて復号化する第２の復号回路とを備えたものである。

【００２７】そして、請求項１７の発明では、前記請求項１６のＬＳＩは、任意の定数が実装可能なヒューズ回路と、前記第２の復号回路の出力を前記ヒューズ回路に実装された定数を用いて暗号化し、第３の被暗号化鍵として当該ＬＳＩ外部に出力する暗号回路と、当該ＬＳＩの第３の入力を、前記ヒューズ回路に実装された定数を用いて復号する第３の復号回路とを備えたものとする。

【００２８】また、請求項１８の発明では、前記請求項１６のＬＳＩは、任意の定数が実装可能なヒューズ回路と、前記ヒューズ回路に実装された定数を前記種生成部から出力された変換種を用いて一方向関数によって変換する第２の一方向関数回路と、前記第２の復号回路の出力を前記第２の一方向関数回路の出力を用いて暗号化し、第３の被暗号化鍵として当該ＬＳＩ外部に出力する暗号回路と、第３の入力を前記第２の一方向関数回路の出力を用いて復号化する第３の復号回路とを備えたものとする。

【００２９】また、請求項１９の発明が講じた解決手段は、システムに鍵を実装する方法として、前記システムが有する記憶部に、最終鍵を、第１の内部鍵を用いて暗号化して得た第１の被暗号化鍵と、第２の内部鍵を、前記第１の被暗号化鍵を用いて暗号化して得た第２の被暗号化鍵とを記憶させる工程と、前記システムにＬＳＩを実装する工程とを備え、前記ＬＳＩは、前記第１の内部鍵を、前記第２の内部鍵を用いて暗号化して得た第３の被暗号化鍵を記憶しており、前記記憶部から、前記第１および第２の被暗号化鍵を入力するものであり、かつ、入力された第２の被暗号化鍵を、入力された第１の被暗号化鍵を鍵として用いて復号化する第１の復号回路と、前記第３の被暗号化鍵を、前記第１の復号回路の出力を鍵として用いて復号化する第２の復号回路と、入力された第１の被暗号化鍵を、前記第２の復号回路の出力を鍵として用いて復号化する第３の復号回路とを備えたものである。

【００３０】また、請求項２０の発明が講じた解決手段は、システムに鍵を実装する方法として、前記システムが有する記憶部に、最終鍵を、内部鍵を用いて暗号化して得た第１の被暗号化鍵と、前記内部鍵を、一方向関数による変換によって得た変換鍵を用いて暗号化して得た第２の被暗号化鍵とを記憶させる工程と、前記システムにＬＳＩを実装する工程とを備え、前記ＬＳＩは、前記記憶部から、前記第１および第２の被暗号化鍵を入力するものであり、かつ、前記変換鍵の生成元である変換種を生成する種生成部と、前記種生成部から出力された変換種を、入力された前記第１の被暗号化鍵を用いて前記一方向関数によって変換し、前記変換鍵を生成する一方向関数回路と、入力された前記第２の被暗号化鍵を、前

記一方向関数回路の出力を鍵として用いて復号化する第１の復号回路と、入力された前記第１の被暗号化鍵を、前記第１の復号回路の出力を鍵として用いて復号化する第２の復号回路とを備えたものである。

【００３１】

【発明の実施の形態】以下、本発明の実施の形態について、図面を参照して説明する。

【００３２】なお、以下の説明において、暗号および復号の処理については、対称暗号を前提とする。「対称暗号」とは、図２０に示すように、Ａを入力としてＢを鍵として用いて暗号化して得た被暗号化鍵をＣとすると、Ｃを入力としてＢを鍵として復号化したものは、Ａとなる特性を持つものである。

【００３３】また、Ｘを鍵Ｙを用いて暗号化して得た被暗号化鍵のことを、ＥＸ（Ｙ）と表現するものとする。

【００３４】（第１の実施形態）図１は本発明の第１の実施形態に係る鍵実装システムの構成を示す図である。図１において、本実施形態に係る鍵実装システム１は、記憶部１ａとＬＳＩ１０とを備えている。記憶部１ａは、最終鍵ＤＫ１を、第１の内部鍵ＭＫ１を用いて暗号化して得た第１の被暗号化鍵ＥＤＫ１（ＭＫ１）と、第２の内部鍵ＫＥＹ１を、第１の被暗号化鍵ＥＤＫ１（ＭＫ１）を用いて暗号化して得た第２の被暗号化鍵ＥＫＥＹ１（ＥＤＫ１（ＭＫ１））とを、記憶している。

【００３５】ＬＳＩ１０は、第１の内部鍵ＭＫ１を、第２の内部鍵ＫＥＹ１を用いて暗号化して得た第３の被暗号化鍵ＥＭＫ１（ＫＥＹ１）を鍵記憶部１１に記憶している。また、第２の入力ＩＮ２を、第１の入力ＩＮ１を鍵として用いて復号化する第１の復号回路１２と、鍵記憶部１１に記憶された第３の被暗号化鍵ＥＭＫ１（ＫＥＹ１）を、第１の復号回路１２の出力を鍵として用いて復号化する第２の復号回路１３と、第１の入力ＩＮ１を、第２の復号回路１３の出力を鍵として用いて復号化する第３の復号回路１４とを備えている。

【００３６】ＬＳＩ１０が鍵実装システム１に実装されると、記憶部１ａに記憶された第１および第２の被暗号化鍵ＥＤＫ１（ＭＫ１），ＥＫＥＹ１（ＥＤＫ１（ＭＫ１））が、それぞれ、第１および第２の入力ＩＮ１，ＩＮ２としてＬＳＩ１０に入力される。

【００３７】このとき、ＬＳＩ１０は次のように動作する。すなわち、第１の復号回路１２は、第２の入力ＩＮ２すなわち第２の被暗号化鍵ＥＫＥＹ１（ＥＤＫ１（ＭＫ１））を、第１の入力ＩＮ１すなわち第１の被暗号化鍵ＥＤＫ１（ＭＫ１）を鍵として用いて復号化する。これにより、第１の復号回路１２から、第２の内部鍵ＫＥＹ１が出力される。第２の復号回路１３は、鍵記憶部１１に記憶された第３の被暗号化鍵ＥＭＫ１（ＫＥＹ１）を、第１の復号回路１２の出力すなわち第２の内部鍵ＫＥＹ１を鍵として用いて復号化する。これにより、第２の復号回路１３から、第１の内部鍵ＭＫ１が出力される。そして、第３の復号回路１４は、第１の入力ＩＮ１すなわち第１の被暗号化鍵ＥＤＫ１（ＭＫ１）を、第２の復号回路１３の出力すなわち第１の内部鍵ＭＫ１を鍵として用いて復号化する。これにより、第３の復号回路１４から、最終鍵ＤＫ１が出力される。

【００３８】このように、第１および第２の被暗号化鍵ＥＤＫ１（ＭＫ１），ＥＫＥＹ１（ＥＤＫ１（ＭＫ１））を記憶する記憶部１ａと、第３の被暗号化鍵ＥＭＫ１（ＫＥＹ１）を記憶するＬＳＩ１０とを組み合わせて実装することによって、最終鍵ＤＫ１が生成される鍵実装システム１を実現することができる。そして、記憶部１ａおよびＬＳＩ１０では、機密鍵が全て暗号化して実装されているので、システム上での解析も困難であり、機密性が高い。

【００３９】また、開発過程においても、生の鍵が存在しないので、開発段階での秘匿性も大幅に向上する。

【００４０】図２は図１における各被暗号化鍵を生成する鍵生成の手順の一例を示す図である。図２に示すように、鍵管理者は、最終鍵ＤＫ１を、任意の第１の内部鍵ＭＫ１を鍵として用いて暗号化し、第１の被暗号化鍵ＥＤＫ１（ＭＫ１）を生成する（Ｓ１１）。次に、第１の内部鍵ＭＫ１を、任意の第２の内部鍵ＫＥＹ１を鍵として用いて暗号化し、第３の被暗号化鍵ＥＭＫ１（ＫＥＹ１）を生成する（Ｓ１２）。さらに、第２の内部鍵ＫＥＹ１を、第１の被暗号化鍵ＥＤＫ１（ＭＫ１）を鍵として用いて暗号化し、第２の被暗号化鍵ＥＫＥＹ１（ＥＤＫ１（ＭＫ１））を生成する（Ｓ１３）。

【００４１】そして、鍵管理者は、第１および第２の被暗号化鍵ＥＤＫ１（ＭＫ１），ＥＫＥＹ１（ＥＤＫ１（ＭＫ１））を機器実装者すなわちシステム１の開発者に提供するとともに、第３の被暗号化鍵ＥＭＫ１（ＫＥＹ１）をＬＳＩ１０の開発者に提供する。このように鍵を生成することによって、開発者に、最終鍵ＤＫ１や第１および第２の内部鍵ＭＫ１，ＫＥＹ１を提供する必要が生じないので、開発段階での鍵の秘匿性も大幅に向上する。

【００４２】システム１の製造時には、記憶部１ａに、第１および第２の被暗号化鍵ＥＤＫ１（ＭＫ１），ＥＫＥＹ１（ＥＤＫ１（ＭＫ１））を記憶させるとともに、ＬＳＩ１０を実装する。

【００４３】（第２の実施形態）図３は本発明の第２の実施形態に係る鍵実装システムの構成を示す図である。図３において、図１と共通の構成要素には、図１と同一の符号を付している。

【００４４】ＬＳＩ２０において、鍵記憶部１１Ａは、第３の被暗号化鍵ＥＭＫ１（ＫＥＹ１）に加えて、第１のテスト用内部鍵ｔｓｔＭＫ１を、第２のテスト用内部鍵ｔｓｔＫＥＹ１を用いて暗号化して得た第４の被暗号化鍵ＥｔｓｔＭＫ１（ｔｓｔＫＥＹ１）をさらに記憶している。

【００４５】また、ＬＳＩ２０には、第１および第２のセレクタ１５，１６が新たに設けられている。セレクタ１５，１６はともに、選択信号が“１”のときは入力Ａを選択する一方、選択信号が“０”のときは入力Ｂを選択する。第１のセレクタ１５は、鍵記憶部１１Ａに記憶された第３および第４の被暗号化鍵ＥＭＫ１（ＫＥＹ１），ＥｔｓｔＭＫ１（ｔｓｔＫＥＹ１）を入力とし、このいずれかを、第１のテスト信号ＴＡに応じて選択出力する。第２の復号回路１３は、第１のセレクタ１５の出力を入力とする。また、第２のセレクタ１６は、第１のセレクタ１５の出力と第２の復号回路１３の出力とを入力とし、このいずれかを、第２のテスト信号ＴＢに応じて選択出力する。第３の復号回路１４は、第２のセレクタ１６の出力を鍵として入力する。

【００４６】ここで、第１および第２のテスト信号ＴＡ，ＴＢをともに“０”に設定する。すなわち、第１および第２のセレクタ１５，１６は、ともに、入力Ｂを選択出力する。これにより、システム２におけるＬＳＩ２０の通常動作が実現される。

【００４７】すなわち、第１の実施形態と同様に、記憶部１ａからＬＳＩ２０に、第１の被暗号化鍵ＥＤＫ１（ＭＫ１）が第１の入力ＩＮ１として、第２の被暗号化鍵ＥＫＥＹ１（ＥＤＫ１（ＭＫ１））が第２の入力ＩＮ２として、それぞれ入力される。第１の復号回路１２は、入力された第２の被暗号化鍵ＥＫＥＹ１（ＥＤＫ１（ＭＫ１））を、入力された第１の被暗号化鍵ＥＤＫ１（ＭＫ１）を鍵として用いて復号化し、第２の内部鍵ＫＥＹ１を生成する。

【００４８】第１のセレクタ１５は、第１のテスト信号ＴＡが“０”であるので、入力Ｂすなわち第３の被暗号化鍵ＥＭＫ１（ＫＥＹ１）を選択出力する。第２の復号回路１３は、第１のセレクタ１５の出力すなわち第３の被暗号化鍵ＥＭＫ１（ＫＥＹ１）を、第２の復号回路１２の出力すなわち第２の内部鍵ＫＥＹ１を鍵として用いて復号化し、第１の内部鍵ＭＫ１を生成する。

【００４９】第２のセレクタ１６は、第２のテスト信号ＴＢが“０”であるので、入力Ｂすなわち、第２の復号回路１３の出力すなわち第１の内部鍵ＭＫ１を選択出力する。第３の復号回路１４は、入力された第１の被暗号化鍵ＥＤＫ１（ＭＫ１）を、第１の内部鍵ＭＫ１を鍵として用いて復号化し、最終鍵ＤＫ１を生成する。すなわち、第１の実施形態と同様の動作が実行される。

【００５０】図３において、第１および第２のテスト信号ＴＡ，ＴＢがともに“０”であるとき以外の場合には、最終鍵ＤＫ１は正常に生成されない。例えばいま、第１および第２のテスト信号ＴＡ，ＴＢはともに“１”に設定されているものとする。

【００５１】第１のセレクタ１５は第１のテスト信号ＴＡを受けて、入力Ａすなわち第４の被暗号化鍵ＥｔｓｔＭＫ１（ｔｓｔＫＥＹ１）を選択出力する。また第２のセレクタ１６は第２のテスト信号ＴＢを受けて、入力Ａすなわち、第１のセレクタ１５の出力すなわち第４の被暗号化鍵ＥｔｓｔＭＫ１（ｔｓｔＫＥＹ１）を選択出力する。このとき、第３の復号回路１４は、入力された第１の被暗号化鍵ＥＤＫ１（ＭＫ１）を、第２のセレクタ１６の出力すなわち第４の被暗号化鍵ＥｔｓｔＭＫ１（ｔｓｔＫＥＹ１）を鍵として復号化する。この結果、第３の復号回路１４から最終鍵ＤＫ１が生成されることはない。

【００５２】図４は本実施形態に係るＬＳＩ２０の開発時におけるテストベンチの構成を示す図である。図４において、テストベンチ２Ｂに設けられたテスト記憶部２ｂには、ＬＳＩ開発用の被暗号化鍵が実装されている。このため、ＬＳＩ開発時には、製品用の鍵を見ることなく開発することができる。

【００５３】すなわち、テスト記憶部２ｂは、鍵ｔｓｔＤＫ１を第３の被暗号化鍵ＥＭＫ１（ＫＥＹ１）を用いて暗号化して得た第１の開発用被暗号化鍵ＥｔｓｔＤＫ１（ＥＭＫ１（ＫＥＹ１））と、鍵ｔｓｔＤＫ１を鍵ｔｓｔＭＫ１を用いて暗号化して得た第２の開発用被暗号化鍵ＥｔｓｔＤＫ１（ｔｓｔＭＫ１）と、第２の開発用被暗号化鍵ＥｔｓｔＤＫ１（ｔｓｔＭＫ１）を用いて鍵ｔｓｔＫＥＹ１を暗号化して得た第３の開発用被暗号化鍵ＥｔｓｔＫＥＹ１（ＥｔｓｔＤＫ１（ｔｓｔＭＫ１））とを、記憶している。ここで、鍵ｔｓｔＤＫ１，ｔｓｔＭＫ１，ｔｓｔＫＥＹ１はいずれも開発用の鍵であり、実際の製品（システム）上では使用されないものとする。

【００５４】また、テストベンチ２Ｂには、第３のセレクタ１７が設けられている。第３のセレクタ１７は、第１の開発用被暗号化鍵ＥｔｓｔＤＫ１（ＥＭＫ１（ＫＥＹ１））を入力Ａ、第２の開発用被暗号化鍵ＥｔｓｔＤＫ１（ｔｓｔＭＫ１）を入力Ｂとし、このいずれかを、第２のテスト信号ＴＢに応じて選択出力する。第３のセレクタ１７の出力は、第１の入力ＩＮ１としてＬＳＩ２０に入力される。

【００５５】図４において、まず、第１～第３の復号回路１２，１３，１４が正常に動作するか否かをテストする。この場合、第１のテスト信号ＴＡを“１”に設定するとともに、第２のテスト信号ＴＢを“０”に設定する。

【００５６】このとき、第３のセレクタ１７は第２のテスト信号ＴＢを受けて、入力Ｂすなわち第２の開発用被暗号化鍵ＥｔｓｔＤＫ１（ｔｓｔＭＫ１）を選択出力する。第１の復号回路１２は、入力ＩＮ２として入力された第３の開発用被暗号化鍵ＥｔｓｔＫＥＹ１（ＥｔｓｔＤＫ１（ｔｓｔＭＫ１））を、第２の開発用被暗号化鍵ＥｔｓｔＤＫ１（ｔｓｔＭＫ１）を鍵として用いて復号化し、第２のテスト用内部鍵ｔｓｔＫＥＹ１を生成する。

【００５７】第１のセレクタ１５は第１のテスト信号ＴＡを受けて、入力Ａすなわち第４の被暗号化鍵ＥｔｓｔＭＫ１（ｔｓｔＫＥＹ１）を選択出力する。第２の復号回路１３は、第２のセレクタ１５の出力すなわち第４の被暗号化鍵ＥｔｓｔＭＫ１（ｔｓｔＫＥＹ１）を、第１の復号回路１２の出力すなわち第２のテスト用内部鍵ｔｓｔＫＥＹ１を鍵として用いて復号化し、第１のテスト用内部鍵ｔｓｔＭＫ１を生成する。第２のセレクタ１６は第２のテスト信号ＴＢを受けて、入力Ｂすなわち、第２の復号回路１３の出力すなわち第１のテスト用内部鍵ｔｓｔＭＫ１を選択出力する。第３の復号回路１４は、入力ＩＮ１すなわち第２の開発用被暗号化鍵ＥｔｓｔＤＫ１（ｔｓｔＭＫ１）を、第２のセレクタ１６の出力すなわち第１のテスト用内部鍵ｔｓｔＭＫ１を鍵として用いて復号化し、テスト用最終鍵ｔｓｔＤＫ１を生成する。

【００５８】次に、実際の製品に使用される第３の被暗号化鍵ＥＭＫ１（ＫＥＹ１）が正しく実装されているか否かをテストする。この場合、第１のテスト信号ＴＡを“０”に設定するとともに、第２のテスト信号ＴＢを“１”に設定する。

【００５９】このとき、第３のセレクタ１７は第２のテスト信号ＴＢを受けて、入力Ａすなわち第１の開発用被暗号化鍵ＥｔｓｔＤＫ１（ＥＭＫ１（ＫＥＹ１））を選択出力する。この第１の開発用被暗号化鍵ＥｔｓｔＤＫ１（ＥＭＫ１（ＫＥＹ１））は、第３の復号回路１４に入力として与えられる。

【００６０】第１のセレクタ１５は第１のテスト信号ＴＡを受けて、入力Ｂすなわち第３の被暗号化鍵ＥＭＫ１（ＫＥＹ１）を選択出力する。第２のセレクタ１６は第２のテスト信号ＴＢを受けて、入力Ａすなわち、第１のセレクタ１５の出力すなわち第３の被暗号化鍵ＥＭＫ１（ＫＥＹ１）を選択出力する。第３の復号回路１４は、第１の開発用被暗号化鍵ＥｔｓｔＤＫ１（ＥＭＫ１（ＫＥＹ１））を、第３の被暗号化鍵ＥＭＫ１（ＫＥＹ１）を鍵として用いて復号化し、テスト用最終鍵ｔｓｔＤＫ１を生成する。すなわち、テスト用最終鍵ｔｓｔＤＫ１が正常に生成されるか否かによって、第３の被暗号化鍵ＥＭＫ１（ＫＥＹ１）が正しく実装されているか否かを判断することができる。

【００６１】図５は図３および図４における各被暗号化鍵を生成する鍵生成の手順の一例を示す図である。図５に示すように、鍵管理者は、最終鍵ＤＫ１を、任意の第１の内部鍵ＭＫ１を鍵として用いて暗号化し、第１の被暗号化鍵ＥＤＫ１（ＭＫ１）を生成する（Ｓ１１）。次に、第１の内部鍵ＭＫ１を、任意の第２の内部鍵ＫＥＹ１を鍵として用いて暗号化し、第３の被暗号化鍵ＥＭＫ１（ＫＥＹ１）を生成する（Ｓ１２）。さらに、第２の内部鍵ＫＥＹ１を、第１の被暗号化鍵ＥＤＫ１（ＭＫ１）を鍵として用いて暗号化し、第２の被暗号化鍵ＥＫＥＹ１（ＥＤＫ１（ＭＫ１））を生成する（Ｓ１３）。

【００６２】そして、鍵管理者は、第１および第２の被暗号化鍵ＥＤＫ１（ＭＫ１），ＥＫＥＹ１（ＥＤＫ１（ＭＫ１））を機器実装者に提供するとともに、第３の被暗号化鍵ＥＭＫ１（ＫＥＹ１）をＬＳＩ２０の開発者に提供する。ここまでは、図２の手順と同様である。

【００６３】これとともに、鍵管理者は、テスト用最終鍵ｔｓｔＤＫ１を、任意の第１のテスト用内部鍵ｔｓｔＭＫ１を用いて暗号化し、第２の開発用被暗号化鍵ＥｔｓｔＤＫ１（ｔｓｔＭＫ１）を生成する（Ｓ２１）。次に、第１のテスト用内部鍵ｔｓｔＭＫ１を、任意の第２のテスト用内部鍵ｔｓｔＫＥＹ１を用いて暗号化し、第４の被暗号化鍵ＥｔｓｔＭＫ１（ｔｓｔＫＥＹ１）を生成する（Ｓ２２）。さらに、第２のテスト用内部鍵ｔｓｔＫＥＹ１を、第２の開発用被暗号化鍵ＥｔｓｔＤＫ１（ｔｓｔＭＫ１）を用いて暗号化し、第３の開発用被暗号化鍵ＥｔｓｔＫＥＹ１（ｔｓｔＥＤＫ１（ｔｓｔＭＫ１））を生成する（Ｓ２３）。そして、テスト用最終鍵ｔｓｔＤＫ１を、第３の被暗号化鍵ＥＭＫ１（ＫＥＹ１）を用いて暗号化し、第１の開発用被暗号化鍵ＥｔｓｔＤＫ１（ＥＭＫ１（ＫＥＹ１））を生成する（Ｓ２４）。

【００６４】そして、鍵管理者は、第４の被暗号化鍵ＥｔｓｔＭＫ１（ｔｓｔＫＥＹ１）、並びに、第１～第３の開発用被暗号化鍵ＥｔｓｔＤＫ１（ＥＭＫ１（ＫＥＹ１）），ＥｔｓｔＤＫ１（ｔｓｔＭＫ１）およびＥｔｓｔＫＥＹ１（ＥｔｓｔＤＫ１（ｔｓｔＭＫ１））をＬＳＩ２０の開発者に提供する。

【００６５】（第３の実施形態）図６は本発明の第３の実施形態に係る鍵実装システムの構成を示す図である。図６において、本実施形態に係る鍵実装システム３は、記憶部３ａとＬＳＩ３０とを備えている。記憶部３ａは、最終鍵ＤＫ１を、内部鍵ＭＫ１を用いて暗号化して得た第１の被暗号化鍵ＥＤＫ１（ＭＫ１）と、内部鍵ＭＫ１を、一方向関数による変換によって得た変換鍵ＣＫ１を用いて暗号化して得た第２の被暗号化鍵ＥＭＫ１（ＣＫ１）とを、記憶している。

【００６６】ＬＳＩ３０は、任意の定数Ｃｏｎｓｔ１を記憶する定数記憶部３１ａを備えている。この定数記憶部３１ａによって種生成部３１が構成されており、変換鍵ＣＫ１を生成するための元になる変換種として定数Ｃｏｎｓｔ１は出力される。また、変換種となる定数Ｃｏｎｓｔ１を、第１の入力ＩＮ１を用いて一方向関数によって変換し、変換鍵ＣＫ１を生成する一方向関数回路３２と、第２の入力ＩＮ２を、一方向関数回路３２の出力を鍵として用いて復号化する第１の復号回路３３と、第１の入力ＩＮ１を、第１の復号回路３３の出力を鍵として用いて復号化する第２の復号回路３４とを備えている。

【００６７】ＬＳＩ３０が鍵実装システム３に実装され

ると、記憶部３ａに記憶された第１および第２の被暗号化鍵ＥＤＫ１（ＭＫ１），ＥＭＫ１（ＣＫ１）が、それぞれ、第１および第２の入力ＩＮ１，ＩＮ２としてＬＳＩ３０に入力される。

【００６８】このとき、ＬＳＩ３０は次のように動作する。すなわち、一方向関数回路３２は、定数記憶部３１ａから出力された定数Ｃｏｎｓｔ１を、第１の入力ＩＮ１すなわち第１の被暗号化鍵ＥＤＫ１（ＭＫ１）を用いて、変換鍵ＣＫ１の生成に用いたものに相当する一方向関数によって変換する。これにより、一方向関数回路３２から、変換鍵ＣＫ１が生成出力される。第１の復号回路３３は、第２の入力ＩＮ２すなわち第２の被暗号化鍵ＥＭＫ１（ＣＫ１）を、一方向関数回路３２の出力すなわち変換鍵ＣＫ１を鍵として用いて復号化する。これにより、第１の復号回路３３から、内部鍵ＭＫ１が生成出力される。第２の復号回路３４は、第１の入力ＩＮ１すなわち第１の被暗号化鍵ＥＤＫ１（ＭＫ１）を、第１の復号回路３３の出力すなわち内部鍵ＭＫ１を鍵として用いて復号化する。これにより、第２の復号回路３４から、最終鍵ＤＫ１が生成される。

【００６９】ここで、例えば、内部鍵ＭＫ１をＭＫ２に変更するものとする。この場合、記憶部３ａには、まず、最終鍵ＤＫ１を新たな内部鍵ＭＫ２を用いて暗号化して得た第１の被暗号化鍵ＥＤＫ１（ＭＫ２）を記憶させる。また、ＬＳＩ３０の定数記憶部３１ａに記憶された任意の定数Ｃｏｎｓｔ１を、第１の被暗号化鍵ＥＤＫ１（ＭＫ２）を鍵として用いて一方向関数によって変換し、新たな変換鍵ＣＫ２を生成する。そして、新たな内部鍵ＭＫ２を、新たな変換鍵ＣＫ２を用いて暗号化して得た第２の被暗号化鍵ＥＭＫ２（ＣＫ２）を、記憶部３ａに記憶させる。

【００７０】このようにして記憶部３ａに記憶させる第１および第２の被暗号化鍵を設定したとしても、上述したのと同様の動作によって、最終鍵ＤＫ１が正しく生成される。すなわち、ＬＳＩ３０に記憶された定数Ｃｏｎｓｔ１を変更することなく、システム３内に記憶させる被暗号化鍵を、任意に設定することが可能になる。これにより、共通のＬＳＩを用いて、システム毎に個別に、暗号化する鍵を設定することができ、このため、機密性をより高いものにすることができる。

【００７１】図７は図６における各被暗号化鍵を生成する鍵生成の手順の一例を示す図である。図７に示すように、鍵管理者は、最終鍵ＤＫ１を、任意の内部鍵ＭＫ１を鍵として用いて暗号化し、第１の被暗号化鍵ＥＤＫ１（ＭＫ１）を生成する（Ｓ３１）。次に、定数Ｃｏｎｓｔ１を、第１の被暗号化鍵ＥＤＫ１（ＭＫ１）を鍵入力として用いて一方向関数による変換を行い、変換鍵ＣＫ１を生成する（Ｓ３２）。その後、内部鍵ＭＫ１を、変換鍵ＣＫ１を鍵として用いて暗号化し、第２のＥＭＫ１（ＣＫ１）を生成する（Ｓ３３）。そして、鍵管理者は、第１および第２の被暗号化鍵ＥＤＫ１（ＭＫ１），ＥＭＫ１（ＣＫ１）を機器実装者すなわちシステム３の開発者に提供するとともに、定数Ｃｏｎｓｔ１をＬＳＩ３０の開発者に提供する。

【００７２】システム３の製造時には、記憶部３ａに、第１および第２の被暗号化鍵ＥＤＫ１（ＭＫ１），ＥＭＫ１（ＣＫ１）を記憶させるとともに、ＬＳＩ３０を実装する。

【００７３】（第４の実施形態）図８は本発明の第４の実施形態に係る鍵実装システムの構成を示す図である。図８において、図６と共通の構成要素には、図６と同一の符号を付している。本実施形態に係る鍵実装システム４は、記憶部４ａとＬＳＩ４０とを備えている。記憶部４ａは、第３の実施形態で説明した第１および第２の被暗号化鍵ＥＤＫ１（ＭＫ１），ＥＭＫ１（ＣＫ１）に加えて、第１の定数ＩＤ１をさらに記憶している。

【００７４】一方、ＬＳＩ４０は、図６に示すＬＳＩ３０における種生成部３１に代えて、定数記憶部４２と、第２の一方向関数回路４３とからなる種生成部４１を備えている。定数記憶部４２は第２の定数Ｃｏｎｓｔ２を記憶しており、第２の一方向関数回路４３は第２の定数Ｃｏｎｓｔ２を、第３の入力ＩＮ３を用いて一方向関数によって変換する。第２の一方向関数回路４３の出力は、変換種として、一方向関数回路３２に与えられる。

【００７５】ＬＳＩ４０が鍵実装システム４に実装されると、記憶部４ａに記憶された第１および第２の被暗号化鍵ＥＤＫ１（ＭＫ１），ＥＭＫ１（ＣＫ１）並びに第１の定数ＩＤ１が、それぞれ、第１～第３の入力ＩＮ１，ＩＮ２，ＩＮ３としてＬＳＩ４０に入力される。

【００７６】このとき、ＬＳＩ４０は次のように動作する。すなわち、種生成部４１内の第２の一方向関数回路４３は、定数記憶部３１ａから出力された定数Ｃｏｎｓｔ２を、第３の入力ＩＮ３すなわち第１の定数ＩＤ１を用いて一方向関数によって変換する。これにより、種生成部４１から、変換種Ｃｏｎｓｔ１が生成出力される。一方向関数回路３２は、種生成部４１から出力された変換種Ｃｏｎｓｔ１を、第１の入力ＩＮ１すなわち第１の被暗号化鍵ＥＤＫ１（ＭＫ１）を用いて、変換鍵ＣＫ１の生成に用いたものに相当する一方向関数によって変換する。これにより、一方向関数回路３２から、変換鍵ＣＫ１が生成出力される。以降、第１および第２の復号回路３３，３４の動作は、第３の実施形態と同様である。

【００７７】図９は図８における各被暗号化鍵を生成する鍵生成の手順の一例を示す図である。図９に示すように、鍵管理者は、最終鍵ＤＫ１を、任意の内部鍵ＭＫ１を鍵として用いて暗号化し、第１の被暗号化鍵ＥＤＫ１（ＭＫ１）を生成する（Ｓ４１）。次に、第２の定数Ｃｏｎｓｔ２を、第１の定数ＩＤ１を鍵として用いて一方向関数によって変換し（Ｓ４２）、さらにその変換結果を、第１の被暗号化鍵ＥＤＫ１（ＭＫ１）を鍵として用

いて一方向関数によって変換し、変換鍵ＣＫ１を生成する（Ｓ４３）。その後、内部鍵ＭＫ１を変換鍵ＣＫ１を鍵として用いて暗号化し、第２の被暗号化鍵ＥＭＫ１（ＣＫ１）を生成する（Ｓ４４）。そして、鍵管理者は、第１の定数ＩＤ１と、第１および第２の被暗号化鍵ＥＤＫ１（ＭＫ１），ＥＭＫ１（ＣＫ１）を機器実装者すなわちシステム４の開発者に提供するとともに、第２の定数Ｃｏｎｓｔ２をＬＳＩ４０の開発者に提供する。

【００７８】（第５の実施形態）図１０は本発明の第５の実施形態に係る鍵実装システムの構成を示す図である。図１０において、図６と共通の構成要素には、図６と同一の符号を付している。本実施形態に係る鍵実装システム５は、記憶部５ａとＬＳＩ５０とを備えている。記憶部５ａは、第３の実施形態で説明した第１および第２の被暗号化鍵ＥＤＫ１（ＭＫ１），ＥＭＫ１（ＣＫ１）に加えて、第１の定数ＩＤ１を、第１の被暗号化鍵ＥＤＫ１（ＭＫ１）を用いて暗号化して得た第３の被暗号化鍵ＥＤＫ１（ＭＫ１）をさらに記憶している。

【００７９】一方、ＬＳＩ５０は、図６に示すＬＳＩ３０における種生成部３１に代えて、定数記憶部５２と、第３および第４の復号回路５３，５４とからなる種生成部５１を備えている。第３の復号回路５３は第３の入力ＩＮ３を、第１の入力ＩＮ１を鍵として用いて復号化する。定数記憶部５２は、変換鍵ＣＫ１の生成元である変換種Ｃｏｎｓｔ１を第１の定数ＩＤ１を用いて暗号化して得た第４の被暗号化鍵ＥＣｏｎｓｔ１（ＩＤ１）を記憶する。第４の復号回路５４は第４の被暗号化鍵ＥＣｏｎｓｔ１（ＩＤ１）を、第３の復号回路５３の出力を鍵として用いて復号化する。第４の復号回路５４の出力は、変換種として、一方向関数回路３２に与えられる。

【００８０】ＬＳＩ５０が鍵実装システム５に実装されると、記憶部５ａに記憶された第１～第３の被暗号化鍵ＥＤＫ１（ＭＫ１），ＥＭＫ１（ＣＫ１），ＥＩＤ１（ＥＤＫ１（ＭＫ１））が、それぞれ、第１～第３の入力ＩＮ１，ＩＮ２，ＩＮ３としてＬＳＩ５０に入力される。

【００８１】このとき、ＬＳＩ５０は次のように動作する。すなわち、種生成部５１内の第３の復号回路５３は、第３の入力ＩＮ３すなわち第３の被暗号化鍵ＥＩＤ１（ＥＤＫ１（ＭＫ１））を、第１の入力ＩＮ１すなわち第１の被暗号化鍵ＥＤＫ１（ＭＫ１）を鍵として用いて復号化する。これにより、第３の復号回路５３から、第１の定数ＩＤ１が出力される。種生成部５１内の第４の復号回路５４は、定数記憶部５２に記憶された第４の被暗号化鍵ＥＣｏｎｓｔ１（ＩＤ１）を、第３の復号回路５３の出力すなわち第１の定数ＩＤ１を鍵として用いて復号化する。これにより、種生成部５１から、変換種Ｃｏｎｓｔ１が生成出力される。一方向関数回路３２は、種生成部５１から出力された変換種Ｃｏｎｓｔ１を、第１の入力ＩＮ１すなわち第１の被暗号化鍵ＥＤＫ１（ＭＫ１）を用いて、変換鍵ＣＫ１の生成に用いたものに相当する一方向関数によって変換する。これにより、一方向関数回路３２から、変換鍵ＣＫ１が生成出力される。以降、第１および第２の復号回路３３，３４の動作は、第３の実施形態と同様である。

【００８２】図１１は図１０における各被暗号化鍵を生成する鍵生成の手順の一例を示す図である。図１１に示すように、鍵管理者は、最終鍵ＤＫ１を、任意の内部鍵ＭＫ１を鍵として用いて暗号化し、第１の被暗号化鍵ＥＤＫ１（ＭＫ１）を生成する（Ｓ５１）。次に、変換種となる定数Ｃｏｎｓｔ１を、第１の定数ＩＤ１を鍵として用いて暗号化し、第４の被暗号化鍵ＥＣｏｎｓｔ１（ＩＤ１）を生成する（Ｓ５２）。また、定数Ｃｏｎｓｔ１を、第１の被暗号化鍵ＥＤＫ１（ＭＫ１）を用いて一方向関数によって変換し、変換鍵ＣＫ１を生成する（Ｓ５３）。その後、内部鍵ＭＫ１を最終鍵ＣＫ１を鍵として用いて暗号化し、第２の被暗号化鍵ＥＭＫ１（ＣＫ１）を生成する（Ｓ５４）。そして、鍵管理者は、第１～第３の被暗号化鍵ＥＤＫ１（ＭＫ１），ＥＭＫ１（ＣＫ１），ＥＩＤ１（ＥＤＫ１（ＭＫ１））を機器実装者すなわちシステム５の開発者に提供するとともに、第４の被暗号化鍵ＥＣｏｎｓｔ１（ＩＤ１）をＬＳＩ５０の開発者に提供する。

【００８３】（第６の実施形態）図１２は本発明の第６の実施形態に係る鍵実装システムの構成を示す図である。図１２において、図６と共通の構成要素には、図６と同一の符号を付している。本実施形態に係る鍵実装システム６は、記憶部６ａとＬＳＩ６０とを備えている。記憶部６ａは、第３の実施形態で説明した第１および第２の被暗号化鍵ＥＤＫ１（ＭＫ１），ＥＭＫ１（ＣＫ１）に加えて、内部鍵ＭＫ１を、テスト用変換鍵ｔｓｔＣＫ１を鍵として用いて暗号化して得た第３の被暗号化鍵ＥＭＫ１（ｔｓｔＣＫ）を記憶している。テスト用変換鍵ｔｓｔＣＫ１は、変換鍵ＣＫ１の生成に用いられたものと同等の一方向関数によって変換されたものである。

【００８４】一方、ＬＳＩ６０は、図６に示すＬＳＩ３０といくつかの点で異なっている。

【００８５】まず、第２および第３の入力ＩＮ２，ＩＮ３を入力とし、このいずれかを、テスト信号ＴＥＳＴに応じて選択出力する第１のセレクタ６４を備えている。第１の復号回路３３は、この第１のセレクタ６４の出力を入力とする。

【００８６】またＬＳＩ６０は、図６における種生成部３１に代えて、定数記憶部６２と、第２のセレクタ６３とからなる種生成部６１を備えている。定数記憶部６２は、変換鍵ＣＫ１の生成元である変換種ＩＤｆｕｓｅ１と、テスト変換鍵ｔｓｔＣＫ１の生成元であるテスト変換種ｔｓｔＩＤ１とを記憶している。定数記憶部６２は、定数Ｉｄｆｕｓｅ１として、レーザトリミング等に

よるヒューズ切断により任意の値が実装可能に構成されている。第2のセレクタ63は、変換種IDfuse1およびテスト変換種tstID1のいずれかを、テスト信号TESTに応じて選択出力する。第2のセレクタ63の出力は、変換種として、一方向関数回路32に与えられる。

【0087】またLSI60には、第2のセレクタ63の出力を検証する検証回路65が設けられている。検証回路65は、定数IDfuse1に対する冗長演算の結果に相当する定数CRCfuse1がヒューズ実装された定数記憶部66と、第2のセレクタ63の出力に対して上述の冗長演算を行い、その結果と定数記憶部66に記憶された定数CRCfuse1とを比較する比較回路67とを備えている。

【0088】LSI60が鍵実装システム6に実装されると、記憶部6aに記憶された第1～第3の被暗号化鍵EDK1（MK1），EMK1（CK1），EMK1（tstCK1）が、それぞれ、第1～第3の入力IN1，IN2，IN3としてLSI60に入力される。

【0089】まず、LSI60の検査時における動作について説明する。この場合、テスト信号TESTは“1”に設定する。

【0090】このとき、第1のセレクタ64はテスト信号TESTとして“1”を受けて、入力IN3すなわち第3の被暗号化鍵EMK1（tstCK1）を選択出力する。また第2のセレクタ63は、テスト信号TESTとして“1”を受けて、定数記憶部62に記憶されたテスト用変換種tstID1を選択出力する。すなわち、種生成部61から、変換種としてテスト用変換種tstID1が出力される。

【0091】そして、一方向関数回路32は、種生成部61から出力されたテスト用変換種tstID1を、第1の入力IN1すなわち第1の被暗号化鍵EDK1（MK1）を用いて、変換鍵CK1およびテスト用変換鍵tstCK1の生成に用いたものに相当する一方向関数によって変換する。これにより、一方向関数回路32から、テスト用変換鍵tstCK1が生成出力される。

【0092】第1の復号回路33は、第1のセレクタ64の出力すなわち第3の被暗号化鍵EMK1（tstCK1）を、一方向関数回路32の出力すなわちテスト変換鍵tstCK1を鍵として用いて復号化する。これにより、第1の復号回路33から、内部鍵MK1が出力される。第2の復号回路34は、第1の入力IN1すなわち第1の被暗号化鍵EDK1（MK1）を、第1の復号回路33の出力すなわち内部鍵MK1を鍵として用いて復号化し、最終鍵DK1を生成する。

【0093】次に、LSI60の通常時における動作について説明する。この場合、テスト信号TESTは“0”に設定する。

【0094】このとき、第1のセレクタ64はテスト信号TESTとして“0”を受けて、入力IN2すなわち第2の被暗号化鍵EMK1（CK1）を選択出力する。また第2のセレクタ63は、テスト信号TESTとして“0”を受けて、定数記憶部62に記憶された変換種IDfuse1を選択出力する。すなわち、種生成部61から、変換種IDfuse1が出力される。

【0095】そして、一方向関数回路32は、種生成部61から出力された変換種IDfuse1を、第1の被暗号化鍵EDK1（MK1）を用いて一方向関数によって変換する。これにより、一方向関数回路32から、変換鍵CK1が生成出力される。第1の復号回路33は、第1のセレクタ64の出力すなわち第2の被暗号化鍵EMK1（CK1）を、一方向関数回路32の出力すなわち変換鍵CK1を鍵として用いて復号化する。これにより、第1の復号回路33から内部鍵MK1が出力され、さらに検査時と同様に、第2の復号回路34から最終鍵DK1が生成される。

【0096】またこのとき、第2のセレクタ63の出力は、検証回路65内の比較回路67にも入力される。比較回路67によって、第2のセレクタ63の出力に対する冗長演算の結果と、定数記憶部66にヒューズ実装された定数CRCfuse1とが同一であるか否かがチェックされる。これにより、種生成部61に記憶された変数種IDfuse1の値の正当性も、併せて検証することができる。

【0097】図13は図12における各暗号化鍵を生成する鍵生成の手順の一例を示す図である。図13に示すように、鍵管理者は、最終鍵DK1を、任意の内部鍵MK1を鍵として用いて暗号化し、第1の被暗号化鍵EDK1（MK1）を生成する（S61）。次に、変換種となる定数IDfuse1を、第1の被暗号化鍵EDK1（MK1）を鍵として用いて一方向関数によって変換し、変換鍵CK1を生成する（S62）。また、定数IDfuse1を冗長演算（例えばCRC16）し、検証用の定数CRCfuse1を生成する（S63）。その後、内部鍵MK1を、変換鍵CK1を鍵として用いて暗号化し、第2の被暗号化鍵EMK1（CK1）を生成する（S64）。

【0098】同様に、テスト用変換種となる定数tstID1を、第1の被暗号化鍵EDK1（MK1）を鍵して用いて一方向関数によって変換し、テスト変換鍵tstCK1を生成する（S62）。その後、内部鍵MK1を、テスト変換鍵tstCK1を鍵として用いて暗号化し、第3の被暗号化鍵EMK1（tstCK1）を生成する（S64）。そして、鍵管理者は、第1～第3の被暗号化鍵EDK1（MK1），EMK1（CK1），EMK1（tstCK1）を機器実装者すなわちシステム6の開発者に提供するとともに、テスト用変換種tstID1，変換種IDfuse1，検証用定数CRCfuse12をLSI60の開発者に提供する。

【００９９】（第７の実施形態）図１４は本発明の第７の実施形態に係る鍵実装システムの構成を示す図である。図１４において、図１２と共通の構成要素には、図１２と同一の符号を付している。本実施形態に係る鍵実装システム７は、図１２と共通の構成からなる記憶部６ａと、ＬＳＩ７０とを備えている。

【０１００】ＬＳＩ７０には、図１２における種生成部６１に代えて、第１の定数記憶部７２と、第２のセレクタ７３と、第２の定数記憶部７４と、第２の一方向関数回路７５とを備えた種生成部７１が設けられている。第１の定数記憶部７２は、変換種ＩＤｆｕｓｅ１の元になる第１の定数ＩＤｆｕｓｅ２と、テスト用変換種ｔｓｔＩＤ１の元になる第２の定数ｔｓｔＩＤ２とを記憶している。第１の定数記憶部７２は、第１の定数ＩＤｆｕｓｅ２として、レーザトリミング等によるヒューズ切断により任意の値が実装可能に構成されている。第２のセレクタ７３は、第１および第２の定数ＩＤｆｕｓｅ２，ｔｓｔＩＤ２のいずれかを、テスト信号ＴＥＳＴに応じて選択出力する。第２の定数記憶部７４は、第３の定数Ｃｏｎｓｔ３を記憶している。第２の一方向関数回路７５は第３の定数Ｃｏｎｓｔ３を、第２のセレクタ７３の出力を用いて、一方向関数によって変換する。

【０１０１】また、検証回路６５の定数記憶部６６には、定数ＣＲＣｆｕｓｅ１の代わりに、第２の定数ＩＤｆｕｓｅ２に対する冗長演算の結果に相当する定数ＣＲＣｆｕｓｅ２がヒューズ実装されている。

【０１０２】まず、ＬＳＩ７０の検査時における動作について説明する。この場合、テスト信号ＴＥＳＴは“１”に設定する。

【０１０３】このとき、第１のセレクタ６４はテスト信号ＴＥＳＴとして“１”を受けて、入力ＩＮ３すなわち第３の被暗号化鍵ＥＭＫ１（ｔｓｔＣＫ１）を選択出力する。また第２のセレクタ７３は、テスト信号ＴＥＳＴとして“１”を受けて、第１の定数記憶部７２に記憶された第２の定数ｔｓｔＩＤ２を選択出力する。第２の一方向関数回路７５は、第２の定数記憶部７４に記憶された第３の定数Ｃｏｎｓｔ３を、第２のセレクタ７３の出力すなわち第２の定数ｔｓｔＩＤ２を用いて一方向関数によって変換する。すなわち、種生成部７１から、変換種としてテスト用変換種ｔｓｔＩＤ１が出力される。

【０１０４】そして、一方向関数回路３２は、種生成部７１から出力されたテスト用変換種ｔｓｔＩＤ１を、第１の入力ＩＮ１すなわち第１の被暗号化鍵ＥＤＫ１（ＭＫ１）を用いて、一方向関数によって変換する。以降の動作は、上述の第６の実施形態と同様である。

【０１０５】次に、ＬＳＩ７０の通常時における動作について説明する。この場合、テスト信号ＴＥＳＴは“０”に設定する。

【０１０６】このとき、第１のセレクタ６４はテスト信号ＴＥＳＴとして“０”を受けて、入力ＩＮ２すなわち第２の被暗号化鍵ＥＭＫ１（ＣＫ１）を選択出力する。また第２のセレクタ７３は、テスト信号ＴＥＳＴとして“０”を受けて、第１の定数記憶部７２に記憶された第１の定数ＩＤｆｕｓｅ２を選択出力する。第２の一方向関数回路７５は、第２の定数記憶部７４に記憶された第１の定数Ｃｏｎｓｔ３を、第２のセレクタ７３の出力すなわち第１の定数ＩＤｆｕｓｅ２を用いて一方向関数によって変換する。これにより、種生成部７１から、変換種ＩＤｆｕｓｅ１が出力される。

【０１０７】そして、一方向関数回路３２は、種生成部７１から出力された変換種ＩＤｆｕｓｅ１を、第１の被暗号化鍵ＥＤＫ１（ＭＫ１）を用いて一方向関数によって変換する。以降の動作は、上述の第６の実施形態と同様である。

【０１０８】またこのとき、第２のセレクタ７３の出力は、検証回路６５内の比較回路６７にも入力される。比較回路６７によって、第２のセレクタ７３の出力に対する冗長演算の結果と、定数記憶部６６にヒューズ実装されたＣＲＣｆｕｓｅ２とが同一であるか否かがチェックされる。これにより、種生成部７１に記憶された第２の定数ＩＤｆｕｓｅ２の正当性も、併せて検証することができる。

【０１０９】図１５は図１４における被暗号化鍵を生成する手順を示す図である。図１５に示すように、鍵管理者は、最終鍵ＤＫ１を、任意の内部鍵ＭＫ１を鍵として用いて暗号化し、第１の被暗号化鍵ＥＤＫ１（ＭＫ１）を生成する（Ｓ７１）。次に、第３の定数ｃｏｎｓｔ３を、第１の定数ＩＤｆｕｓｅ２を鍵として用いて一方向関数によって変換し（Ｓ７２）、さらにその変換結果を、第１の被暗号化鍵ＥＤＫ１（ＭＫ１）を鍵として用いて一方向関数によって変換し、変換鍵ＣＫ１を生成する（Ｓ７３）。その後、内部鍵ＭＫ１を変換鍵ＣＫ１を鍵として用いて暗号化し、第２の被暗号化鍵ＥＭＫ１（ＣＫ１）を生成する（Ｓ７４）。また、第１の定数ＩＤｆｕｓｅ２に対して冗長演算（例えばＣＲＣ１６）を行い、定数ＣＲＣｆｕｓｅ２を生成する（Ｓ７５）。

【０１１０】同様に、第３の定数Ｃｏｎｓｔ３を、第２の定数ｔｓｔＩＤ２を鍵として用いて一方向関数によって変換し（Ｓ７２）、さらにその変換結果を、第１の被暗号化鍵ＥＤＫ１（ＭＫ１）を鍵として用いて一方向関数によって変換し、テスト用変換鍵ｔｓｔＣＫ１を生成する（Ｓ７３）。その後、内部鍵ＭＫ１をテスト用変換鍵ｔｓｔＣＫ１を鍵として用いて暗号化し、第３の被暗号化鍵ＥＭＫ１（ｔｓｔＣＫ１）を生成する。

【０１１１】そして、鍵管理者は、第１～第３の被暗号化鍵ＥＤＫ１（ＭＫ１），ＥＭＫ１（ＣＫ１），ＥＭＫ１（ｔｓｔＣＫ１）をシステム７の開発者に提供するとともに、第１～第３の定数ＩＤｆｕｓｅ２，ｔｓｔＩＤ２，Ｃｏｎｓｔ３と検証用定数ＣＲＣｆｕｓｅ２をＬＳＩ７０の開発者に提供する。

【０１１２】（第８の実施形態）図１６は本発明の第８の実施形態に係る鍵実装システムの構成を示す図である。図１６において、図１２と共通の構成要素には、図１２と同一の符号を付している。本実施形態に係る鍵実装システム８は、図１２と共通の構成からなる記憶部６ａと、ＬＳＩ８０とを備えている。

【０１１３】ＬＳＩ８０には、図１２における種生成部６１に代えて、第１の定数記憶部８２と、第２のセレクタ８３と、第３の復号回路８４と、第２の定数記憶部８５と、第２の一方向関数回路８６とを備えた種生成部８１が設けられている。第１の定数記憶部８２は、第１の定数ＩＤｆｕｓｅ２を、第１の被暗号化鍵ＥＤＫ１（ＭＫ１）を用いて暗号化して得た第４の被暗号化鍵ＥＩＤｆｕｓｅ２（ＥＤＫ１（ＭＫ１））と、第２の定数ｔｓｔＩＤ２を、第１の被暗号化鍵ＥＤＫ１（ＭＫ１）を用いて暗号化して得た第５の被暗号化鍵ＥｔｓｔＩＤ２（ＥＤＫ１（ＭＫ１））とを記憶している。第２のセレクタ８３は、第４および第５の被暗号化鍵ＥＩＤｆｕｓｅ２（ＥＤＫ１（ＭＫ１）），ＥｔｓｔＩＤ２（ＥＤＫ１（ＭＫ１））のいずれかを、テスト信号ＴＥＳＴに応じて選択出力する。第３の復号回路８４は、第２のセレクタ８３の出力を、第１の入力ＩＮ１すなわち第１の被暗号化鍵ＥＤＫ１（ＭＫ１）を鍵として用いて復号化する。第２の定数記憶部８５は第３の定数Ｃｏｎｓｔ３を記憶している。第２の一方向関数回路８６は第３の定数Ｃｏｎｓｔ３を、第３の復号回路８４の出力を用いて、一方向関数によって変換する。

【０１１４】また、検証回路の定数記憶部６６には、定数ＣＲＣｆｕｓｅ１の代わりに、第４の被暗号化鍵ＥＩＤｆｕｓｅ２（ＥＤＫ１（ＭＫ１）に対する冗長演算の結果に相当する定数ＣＲＣｆｕｓｅ３がヒューズ実装されている。

【０１１５】まず、ＬＳＩ８０の検査時における動作について説明する。この場合、テスト信号ＴＥＳＴは“１”に設定する。

【０１１６】このとき、第１のセレクタ６４はテスト信号ＴＥＳＴとして“１”を受けて、入力ＩＮ３すなわち第３の被暗号化鍵ＥＭＫ１（ｔｓｔＣＫ１）を選択出力する。また第２のセレクタ８３は、テスト信号ＴＥＳＴとして“１”を受けて、第１の定数記憶部８２に記憶された第５の被暗号化鍵ＥｔｓｔＩＤ２（ＥＤＫ１（ＭＫ１））を選択出力する。第３の復号回路８４は、第２のセレクタ８３の出力すなわち第５の被暗号化鍵ＥｔｓｔＩＤ２（ＥＤＫ１（ＭＫ１））を、第１の入力すなわち第１の被暗号化鍵ＥＤＫ１（ＭＫ１）によって復号化する。これにより、第３の復号回路８４から、定数ｔｓｔＩＤ２が出力される。第２の一方向関数回路８６は、第２の定数記憶部８５に記憶された第３の定数Ｃｏｎｓｔ３を、第３の復号回路８４の出力すなわち定数ｔｓｔＩＤ２を用いて一方向関数によって変換する。すなわち、種生成部８１から、変換種としてテスト用変換種ｔｓｔＩＤ１が出力される。

【０１１７】そして、一方向関数回路３２は種生成部８１から出力されたテスト用変換種ｔｓｔＩＤ１を、第１の入力ＩＮ１すなわち第１の被暗号化鍵ＥＤＫ１（ＭＫ１）を用いて、一方向関数によって変換する。以降の動作は、上述の第６の実施形態と同様である。

【０１１８】次に、ＬＳＩ８０の通常時における動作について説明する。この場合、テスト信号ＴＥＳＴは“０”に設定する。

【０１１９】このとき、第１のセレクタ６４はテスト信号ＴＥＳＴとして“０”を受けて、入力ＩＮ２すなわち第２の被暗号化鍵ＥＭＫ１（ＣＫ１）を選択出力する。また第２のセレクタ８３は、テスト信号ＴＥＳＴとして“０”を受けて、第１の定数記憶部８２に記憶された第４の被暗号化鍵ＥＩＤｆｕｓｅ２（ＥＤＫ１（ＭＫ１））を選択出力する。第３の復号回路８４は、第２のセレクタ８３の出力すなわち第４の被暗号化鍵ＥＩＤｆｕｓｅ２（ＥＤＫ１（ＭＫ１））を、第１の被暗号化鍵ＥＤＫ１（ＭＫ１）を鍵として用いて復号化する。これにより、第３の復号回路８４から、定数ＩＤｆｕｓｅ２が出力される。第２の一方向関数回路８６は、第３の定数Ｃｏｎｓｔ３を、第３の復号回路８４の出力すなわち定数ＩＤｆｕｓｅ２を用いて一方向関数によって変換する。これにより、種生成部８１から、変換種ＩＤｆｕｓｅ１が出力される。

【０１２０】そして、一方向関数回路３２は、種生成部８１から出力された変換種ＩＤｆｕｓｅ１を、第１の被暗号化鍵ＥＤＫ１（ＭＫ１）を用いて一方向関数によって変換する。以降の動作は、上述の第６の実施形態と同様である。

【０１２１】またこのとき、第２のセレクタ８３の出力は、検証回路６５内の比較回路６７にも入力される。比較回路６７によって、第２のセレクタ８３の出力に対する冗長演算の結果と、定数記憶部６６にヒューズ実装されたＣＲＣｆｕｓｅ３とが同一であるか否かがチェックされる。これにより、種生成部８１に記憶された第４の被暗号化鍵ＥＩＤｆｕｓｅ２（ＥＤＫ１（ＭＫ１））の正当性も、併せて検証することができる。

【０１２２】図１７は図１６における被暗号化鍵を生成する手順を示す図である。図１７に示すように、鍵管理者は、最終鍵ＤＫ１を、任意の内部鍵ＭＫ１を鍵として用いて暗号化し、第１の被暗号化鍵ＥＤＫ１（ＭＫ１）を生成する（Ｓ８１）。次に、第１および第２の定数ＩＤｆｕｓｅ２，ｔｓｔＩＤ２を、第１の被暗号化鍵ＥＤＫ１（ＭＫ１）を鍵として用いて暗号化し、第４および第５の被暗号化鍵ＥＩＤｆｕｓｅ２（ＥＤＫ１（ＭＫ１）），ＥｔｓｔＩＤ２（ＥＤＫ１（ＭＫ１））を生成する（Ｓ８２）。また、第３の定数Ｃｏｎｓｔ３を、第１の定数ＩＤｆｕｓｅ２を鍵として用いて一方向関数に

よって変換し（Ｓ８３）、さらにその変換結果を、第１の被暗号化鍵ＥＤＫ１（ＭＫ１）を鍵として用いて一方向関数によって変換し、変換鍵ＣＫ１を生成する（Ｓ８４）。その後、内部鍵ＭＫ１を、変換鍵ＣＫ１を鍵として用いて暗号化し、第２の被暗号化鍵ＥＭＫ１（ＣＫ１）を生成する（Ｓ８５）。また、第４の被暗号化鍵ＥＩＤｆｕｓｅ２（ＥＤＫ１（ＭＫ１））を冗長演算（例えばＣＲＣ１６）し、検証用の定数ＣＲＣｆｕｓｅ３を生成する（Ｓ８６）。

【０１２３】同様に、第３の定数Ｃｏｎｓｔ３を、第２の定数ｔｓｔＩＤ２を鍵として用いて一方向関数によって変換し（Ｓ８３）、さらにその変換結果を、第１の被暗号化鍵ＥＤＫ１（ＭＫ１）を鍵として用いて一方向関数によって変換し、テスト用変換鍵ｔｓｔＣＫ１を生成する（Ｓ８４）。その後、内部鍵ＭＫ１をテスト用変換鍵ｔｓｔＣＫ１を鍵として用いて暗号化し、第３の被暗号化鍵ＥＭＫ１（ｔｓｔＣＫ１）を生成する。

【０１２４】そして、鍵管理者は、第１～第３の被暗号化鍵ＥＤＫ１（ＭＫ１），ＥＭＫ１（ＣＫ１），ＥＭＫ１（ｔｓｔＣＫ１）をシステム８の開発者に提供するとともに、第３の定数Ｃｏｎｓｔ３と、第４および第５の被暗号化鍵ＥｔｓｔＩＤ２（ＥＤＫ１（ＭＫ１））、ＥＩＤｆｕｓｅ２（ＥＤＫ１（ＭＫ１））と、検証用定数ＣＲＣｆｕｓｅ３とをＬＳＩ８０の開発者に提供する。

【０１２５】（第９の実施形態）図１８は本発明の第９の実施形態に係る鍵実装システムの構成を示す図である。図１８において、図６と共通の構成要素には、図６と同一の符号を付している。本実施形態に係る鍵実装システム３Ａは、記憶部３ｂとＬＳＩ３０Ａとを備えている。記憶部３ｂは、図６の記憶部３ａと同様に、最終鍵ＤＫ１を、内部鍵ＭＫ１を用いて暗号化して得た第１の被暗号化鍵ＥＤＫ１（ＭＫ１）と、内部鍵ＭＫ１を、一方向関数による変換によって得た変換鍵ＣＫ１を用いて暗号化して得た第２の被暗号化鍵ＥＭＫ１（ＣＫ１）とを、記憶している。また、ＬＳＩ３０Ａから入力される第３の被暗号化鍵を記憶するための空き領域３８と、イネーブル状態とディセーブル状態とが切り替え可能に構成されたフラグｆｌａｇとを備えている。

【０１２６】ＬＳＩ３０Ａは、図６のＬＳＩ３０の各要素に加えて、任意の定数ＩＤｆｕｓｅが実装可能なヒューズ回路３５と、第２の復号回路３４の出力を、ヒューズ回路３５に実装された定数ＩＤｆｕｓｅを用いて暗号化する暗号回路３６と、記憶部３ｂからの第３の入力ＩＮ３を、ヒューズ回路３５に実装された定数ＩＤｆｕｓｅを用いて復号化する第３の復号回路３７とを備えている。ヒューズ回路３５はレーザトリミング等によるヒューズ切断によって、ＬＳＩ３０Ａ毎に異なる定数が実装可能に構成されている。暗号回路３６の出力は、第３の被暗号化鍵ＥＤＫ１（ＩＤｆｕｓｅ）として記憶部３ｂに送られる。

【０１２７】記憶部３ｂは、ＬＳＩ３０Ａから第３の被暗号化鍵ＥＤＫ１（ＩＤｆｕｓｅ）を受けたとき、この第３の被暗号化鍵ＥＤＫ１（ＩＤｆｕｓｅ）を空き領域３８に格納するとともに、第１および第２の被暗号化鍵ＥＤＫ１（ＭＫ１），ＥＭＫ１（ＣＫ１）を消去する。そして、ＬＳＩ３０Ａに対して第３の入力ＩＮ３として第３の被暗号化鍵ＥＤＫ１（ＩＤｆｕｓｅ）を出力する。また、フラグｆｌａｇは、記憶部３ｂがシステム３Ａに実装されたときはイネーブル状態であり、第１および第２の被暗号化鍵ＥＤＫ１（ＭＫ１），ＥＭＫ１（ＣＫ１）が消去されると、ディセーブル状態になる。

【０１２８】ＬＳＩ３０Ａがシステム３Ａに実装されると、記憶部３ｂから、第１の被暗号化鍵ＥＤＫ１（ＭＫ１）が第１の入力ＩＮ１としてＬＳＩ３０Ａに入力される。一方向関数回路３２は、種生成部３１から出力された変換種Ｃｏｎｓｔ１を、第１の入力ＩＮ１すなわち第１の被暗号化鍵ＥＤＫ１（ＭＫ１）を用いて一方向関数によって変換する。これにより、一方向関数回路３２から、変換鍵ＣＫ１が生成される。

【０１２９】第１の復号回路３３は、第２の入力ＩＮ２すなわち第２の被暗号化鍵ＥＭＫ１（ＣＫ１）を、一方向関数回路３２の出力すなわち変換鍵ＣＫ１を鍵として用いて復号化する。これにより、第１の復号回路３３から、内部鍵ＭＫ１が生成される。第２の復号回路３４は、第１の入力ＩＮ１すなわち第１の被暗号化鍵ＥＤＫ１（ＭＫ１）を、第１の復号回路３３の出力すなわち内部鍵ＭＫ１を鍵として用いて復号化する。これにより、第２の復号回路３４から、最終鍵ＤＫ１が生成される。

【０１３０】この最終鍵ＤＫ１は、暗号回路３６に与えられる。暗号回路３６は、ヒューズ回路３５に実装された任意の定数ＩＤｆｕｓｅを用いて最終鍵ＤＫ１を暗号化し、第３の被暗号化鍵ＥＤＫ１（ＩＤｆｕｓｅ）を生成する。生成された第３の被暗号化鍵ＥＤＫ１（ＩＤｆｕｓｅ）は、記憶部３ｂに書き込まれる。

【０１３１】このとき、第１および第２の被暗号化鍵ＥＤＫ１（ＭＫ１），ＥＭＫ１（ＣＫ１）は記憶部３ｂから消去される。これとともに、フラグｆｌａｇはディセーブル状態になる。

【０１３２】ここまでの処理を製品出荷前に実行しておくと、記憶部３ｂには、ＬＳＩ３０Ａ固有の定数ＩＤｆｕｓｅを用いて最終鍵ＤＫ１を暗号化して得た第３の被暗号化鍵ＥＤＫ１（ＩＤｆｕｓｅ）のみが記憶された状態で、出荷される。もちろん、製品出荷後に、電源を最初に立ち上げたときに、ここまでの処理を実行するようにしてもかまわない。

【０１３３】そして、フラグｆｌａｇがディセーブル状態のとき、記憶部３ｂからＬＳＩ３０Ａに第３の被暗号化鍵ＥＤＫ１（ＩＤｆｕｓｅ）が第３の入力ＩＮ３として出力される。すると、第３の復号回路３７は、この第３の被暗号化鍵ＥＤＫ１（ＩＤｆｕｓｅ）を定数ＩＤｆ

ｕｓｅを鍵として復号化して、最終鍵ＤＫ１を生成する。

【０１３４】このように本実施形態によると、暗号化に用いる定数がＬＳＩ毎に異なる場合であっても、最終鍵の暗号化を容易に実現することができ、機密性を向上させることができる。

【０１３５】なお、鍵生成の手順は、第３の実施形態と同様に、図７に示すように行えばよい。

【０１３６】（第１０の実施形態）図１９は本発明の第１０の実施形態に係る鍵実装システムの構成を示す図である。図１９において、図１８と共通の構成要素には、図１８と同一の符号が付してある。本実施形態に係る鍵実装システム３Ｂは、記憶部３ｂと、ＬＳＩ３０Ｂとを備えている。

【０１３７】ＬＳＩ３０Ｂは、図１８のＬＳＩ３０Ａと比較すると、さらに、第２の一方向関数回路９１およびセレクタ９２を備えている。第２の一方向関数回路９１はヒューズ回路３５に実装された定数ＩＤｆｕｓｅを、種生成部３１から出力された変換種Ｃｏｎｓｔを用いて一方向関数によって変換し、第２の変換種ＩＤｆｕｓｅＣＯＮを生成する。暗号回路３６および第３の復号回路３７は、定数ＩＤｆｕｓｅの代わりに、この第２の変換種ＩＤｆｕｓｅＣＯＮを鍵として用いて、暗号化および復号化を行う。またセレクタ９２は、記憶部３ｂからの第３の入力ＩＮ３および暗号回路３６の出力のうちのいずれか一方を、テスト信号ＴＥＳＴに応じて選択出力する。第３の復号回路３７は、セレクタ９２の出力を入力とする。

【０１３８】まず、実システム上における動作を説明する。実システム上では、テスト信号は“１”に設定する。

【０１３９】この場合、先の第９の実施形態と同様の動作によって、第２の復号回路３４から、最終鍵ＤＫ１が出力される。暗号回路３６は、第２の復号回路３４の出力すなわち最終鍵ＤＫ１を、一方向関数回路９１の出力すなわち第２の変換鍵ＩＤｆｕｓｅＣＯＮを鍵として用いて暗号化し、第３の被暗号化鍵ＥＤＫ１（ＩＤｆｕｓｅＣＯＮ）を生成する。

【０１４０】ＬＳＩ３０Ｂから出力された第３の被暗号化鍵ＥＤＫ１（ＩＤｆｕｓｅＣＯＮ）は、記憶部３ｂの空き領域３８に格納され、さらに、第３の入力ＩＮ３として、ＬＳＩ３０Ｂに出力される。セレクタ９２はテスト信号ＴＥＳＴとして“１”を受けて、第３の入力すなわち記憶部３ｂから出力された第３の被暗号化鍵ＥＤＫ１（ＩＤｆｕｓｅＣＯＮ）を選択出力する。第３の復号回路３７は、セレクタ９２の出力すなわち第３の被暗号化鍵ＥＤＫ１（ＩＤｆｕｓｅＣＯＮ）を、第２の変換鍵ＩＤｆｕｓｅＣＯＮを鍵として用いて復号化し、最終鍵ＤＫ１を生成する。

【０１４１】また、ＬＳＩ３０Ｂの検査時には、テスト信号ＴＥＳＴは“０”に設定する。このとき、先の通常時と同様の動作によって、暗号回路３６から、第３の被暗号化鍵ＥＤＫ１（ＩＤｆｕｓｅＣＯＮ）が生成される。セレクタ９２はテスト信号ＴＥＳＴとして“０”を受けて、入力Ｂすなわち暗号回路３６から出力された第３の被暗号化鍵ＥＤＫ１（ＩＤｆｕｓｅＣＯＮ）を出力する。第３の復号回路３７は、第２の変換鍵ＩＤｆｕｓｅＣＯＮを鍵として用いてこの第３の被暗号化鍵ＥＤＫ１（ＩＤｆｕｓｅＣＯＮ）を復号化し、最終鍵ＤＫ１を生成する。

【０１４２】このように本実施形態によると、個別に異なる鍵が実装されたＬＳＩを検査するときでも、検査パターンを変更することなく検査可能になる。

【０１４３】なお、鍵生成の手順は、第３の実施形態と同様に、図７に示すように行えばよい。

【０１４４】なお、本実施形態において、セレクタ９２を省いてもかまわないし、第９の実施形態に係る図１８の構成において、セレクタ９２を設けてもかまわない。

【０１４５】また、第９および第１０の実施形態において、種生成部は、他の構成、例えば図８、図１０、図１２、図１４、図１６に示すようなものであっても、かまわない。

【０１４６】

【発明の効果】以上のように本発明によると、ＬＳＩ内の鍵とシステム上の鍵とを相互に暗号化することによって、鍵の相互関係と暗号方式の知識がないと解析が困難になるので、システム上において鍵の解析が困難になり、機密性および秘匿性が大幅に向上する。また、ＬＳＩ開発者やシステム開発者は、被暗号化鍵のみを用いて開発することが可能となり、開発時における機密性を向上することができる。さらには、暗号化する鍵を容易に変更可能となり、システム個別に異なる鍵を与えることが容易になるので、機密性をさらに向上させることができる。

【図面の簡単な説明】

【図１】本発明の第１の実施形態に係る鍵実装システムの構成を示す図である。

【図２】図１のシステムで用いられる被暗号化鍵の生成手順の一例を示す図である。

【図３】本発明の第２の実施形態に係る鍵実装システムの構成を示す図である。

【図４】本発明の第２の実施形態に係るシステム開発時の機密鍵実装方法を示す図である。

【図５】図３および図４で用いられる被暗号化鍵の生成手順の一例を示す図である。

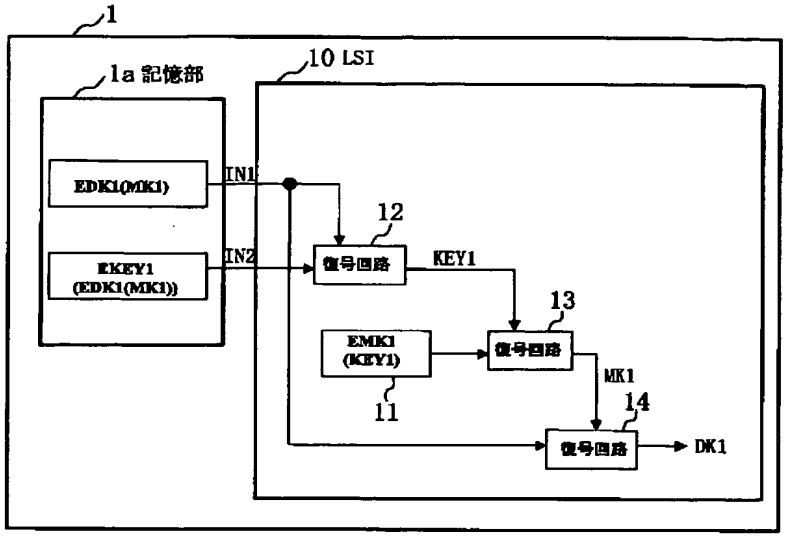
【図６】本発明の第３の実施形態に係る鍵実装システムの構成を示す図である。

【図７】図６のシステムで用いられる被暗号化鍵の生成手順の一例を示す図である。

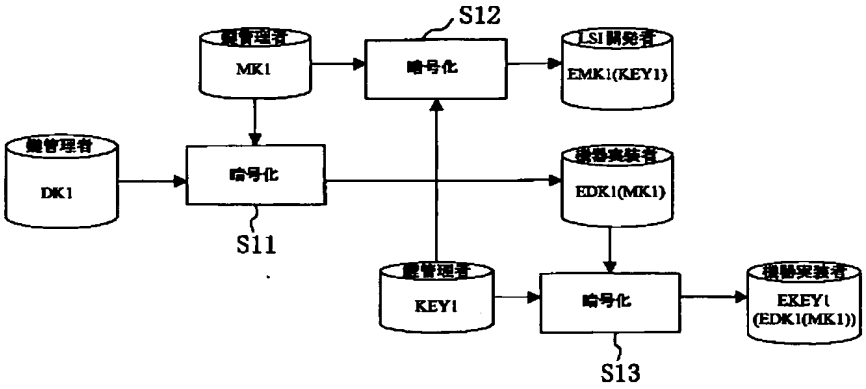
【図８】本発明の第４の実施形態に係る鍵実装システム

の構成を示す図である。
【図９】図８のシステムで用いられる被暗号化鍵の生成手順の一例を示す図である。
【図１０】本発明の第５の実施形態に係る鍵実装システムの構成を示す図である。
【図１１】図１０のシステムで用いられる被暗号化鍵の生成手順の一例を示す図である。
【図１２】本発明の第６の実施形態に係る鍵実装システムの構成を示す図である。
【図１３】図１２のシステムで用いられる被暗号化鍵の生成手順の一例を示す図である。
【図１４】本発明の第７の実施形態に係る鍵実装システムの構成を示す図である。
【図１５】図１４のシステムで用いられる被暗号化鍵の生成手順の一例を示す図である。
【図１６】本発明の第８の実施形態に係る鍵実装システムの構成を示す図である。
【図１７】図１６のシステムで用いられる被暗号化鍵の生成手順の一例を示す図である。
【図１８】本発明の第９の実施形態に係る鍵実装システムの構成を示す図である。
【図１９】本発明の第１０の実施形態に係る鍵実装システムの構成を示す図である。
【図２０】対称暗号を説明するための図である。
【符号の説明】
１，２，３，３Ａ，３Ｂ，４，５，６，７，８　鍵実装システム
１ａ，３ａ，３ｂ，４ａ，５ａ，６ａ　記憶部
１０，２０，３０，３０Ａ，３０Ｂ，４０，５０，６０，７０，８０　ＬＳＩ
１１，１１Ａ　鍵記憶部
１２　第１の復号回路
１３　第２の復号回路
１４　第３の復号回路
１５　第１のセレクタ
１６　第２のセレクタ
３１，４１，５１，６１，７１，８１　種生成部
３１ａ　定数記憶部
３２　一方向関数回路
３３　第１の復号回路
３４　第２の復号回路
３５　ヒューズ回路
３６　暗号回路
３７　第３の復号回路
４２　定数記憶部
４３　第２の一方向関数回路
５２　定数記憶部
５３　第３の復号回路
５４　第４の復号回路
６２　定数記憶部
６３　第２のセレクタ
６４　第１のセレクタ
６５　検証回路
７２　第１の定数記憶部
７３　第２のセレクタ
７４　第２の定数記憶部
７５　第２の一方向関数回路
８２　第１の定数記憶部
８３　第２のセレクタ
８４　第３の復号回路
８５　第２の定数記憶部
８６　第２の一方向関数回路
９１　第２の一方向関数回路
９２　セレクタ
ＤＫ１　最終鍵
ＭＫ１　第１の内部鍵、内部鍵
ＫＥＹ１　第２の内部鍵
ＥＤＫ（ＭＫ１）　第１の被暗号化鍵
ＥＫＥＹ１（ＥＤＫ１（ＭＫ１））　第２の被暗号化鍵
ＥＭＫ１（ＫＥＹ１）　第３の被暗号化鍵
ＥｔｓｔＭＫ１（ｔｓｔＫＥＹ１）　第４の被暗号化鍵
ＥＩＤ１（ＥＤＫ１（ＭＫ１））　第３の被暗号化鍵
ＥＣｏｎｓｔ１（ＩＤ１）　第４の被暗号化鍵
ＥＭＫ１（ｔｓｔＣＫ１）　第３の被暗号化鍵
ＥＩＤｆｕｓｅ２（ＥＤＫ１（ＭＫ１））　第４の被暗号化鍵
ＥｔｓｔＩＤ２（ＥＤＫ１（ＭＫ１））　第５の被暗号化鍵
ＥＤＫ１（ＩＤｆｕｓｅ）　第３の被暗号化鍵
ＥＤＫ１（ＩＤｆｕｓｅＣＯＮ）　第３の被暗号化鍵Ｉ
Ｄｆｕｓｅ１　変換種
ＩＮ１　第１の入力
ＩＮ２　第２の入力
ｔｓｔＭＫ１　第１のテスト用内部鍵
ｔｓｔＫＥＹ１　第２のテスト用内部鍵
ｔｓｔＣＫ１　テスト用変換鍵
ｔｓｔＩＤ１　テスト用変換種
ＴＡ　第１のテスト信号
ＴＢ　第２のテスト信号
ＴＥＳＴ　テスト信号
ＣＫ１　変換鍵
Ｃｏｎｓｔ１　定数（変換種）
ＩＤ１　第１の定数
Ｃｏｎｓｔ２　第２の定数
ＩＤｆｕｓｅ２　第１の定数
ｔｓｔＩＤ２　第２の定数
Ｃｏｎｓｔ３　第３の定数
ＩＤｆｕｓｅ　定数

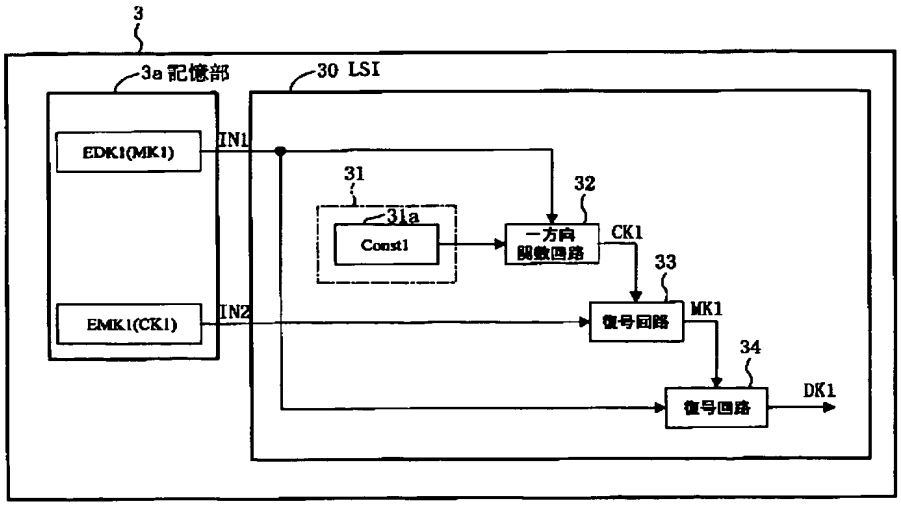
【図1】


1
1a 記憶部
10 LSI
EDK1(MK1)
IN1
12
EKEY1
(EDK1(MK1))
IN2
復号回路
KEY1
13
EMK1
(KEY1)
復号回路
MK1
11
14
復号回路
DK1

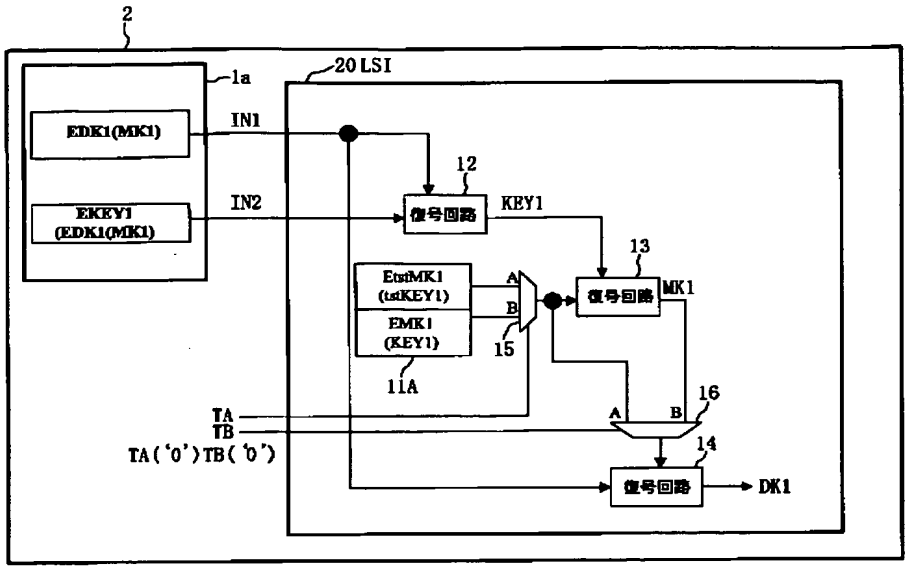
【図2】


S12
MK1
暗号化
EMK1(KEY1)
DK1
暗号化
EDK1(MK1)
S11
KEY1
暗号化
EKEY1
(EDK1(MK1))
S13

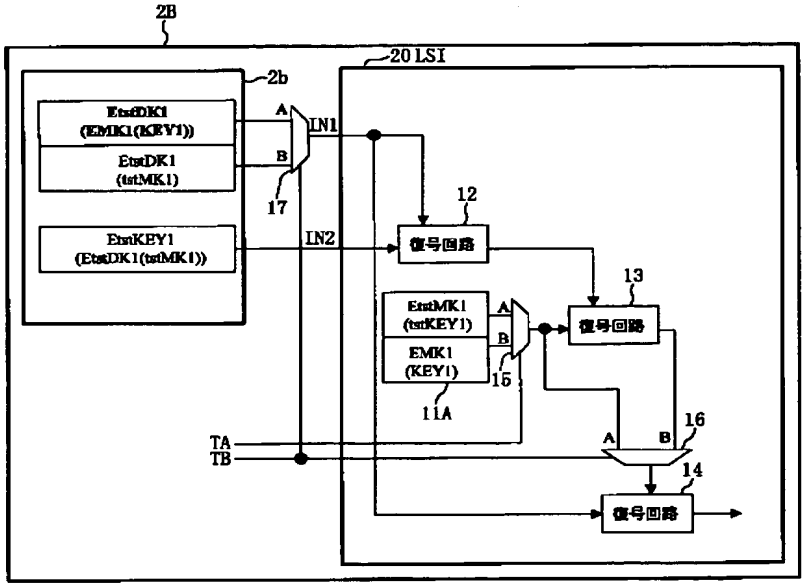
【図6】


3
3a 記憶部
30 LSI
EDK1(MK1)
IN1
31
31a
Const1
32
一方向
関数回路
CK1
33
EMK1(CK1)
IN2
復号回路
MK1
34
復号回路
DK1

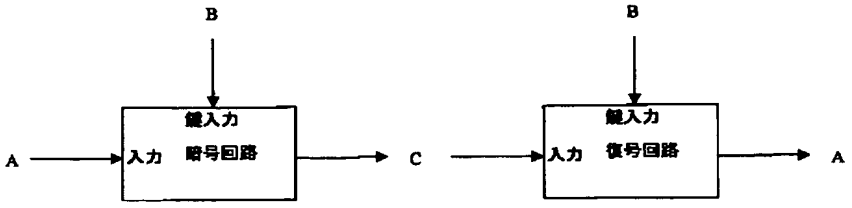
【図3】


2
1a
20 LSI
EDK1(MK1)
IN1
EKEY1
(EDK1(MK1)
IN2
12
復号回路
KEY1
13
EtstMK1
(tstKEY1)
EMK1
(KEY1)
11A
A
B
15
復号回路
MK1
TA
TB
TA('0')TB('0')
16
14
復号回路
DK1

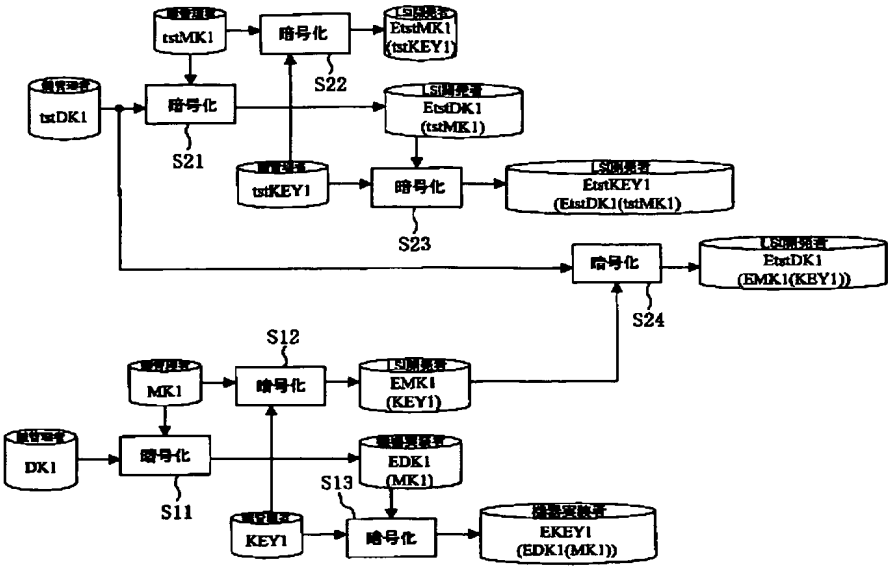
【図4】


2B
20 LSI
2b
EtstDK1
(EMK1(KEY1))
EtstDK1
(tstMK1)
EtstKEY1
(EtstDK1(tstMK1))
A
B
17
IN1
IN2
12
復号回路
13
EtstMK1
(tstKEY1)
EMK1
(KEY1)
11A
15
復号回路
TA
TB
16
14
復号回路

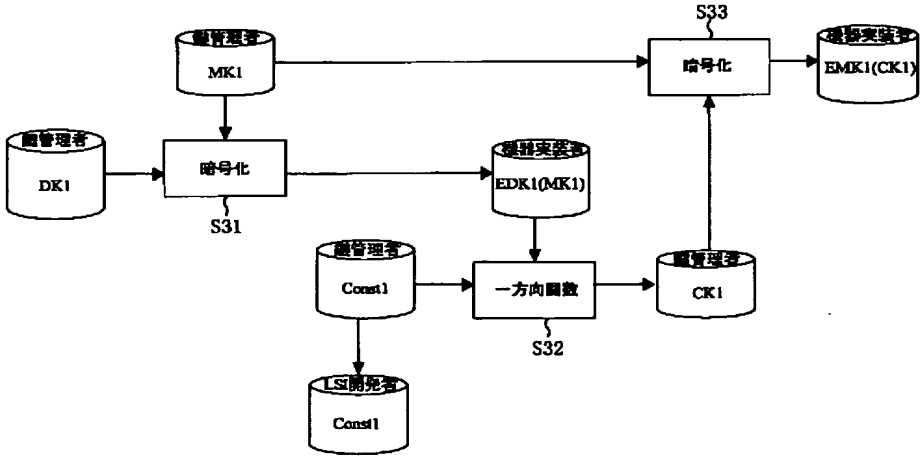
【図20】


B
鍵入力
A
入力
暗号回路
C
B
鍵入力
入力
復号回路
A

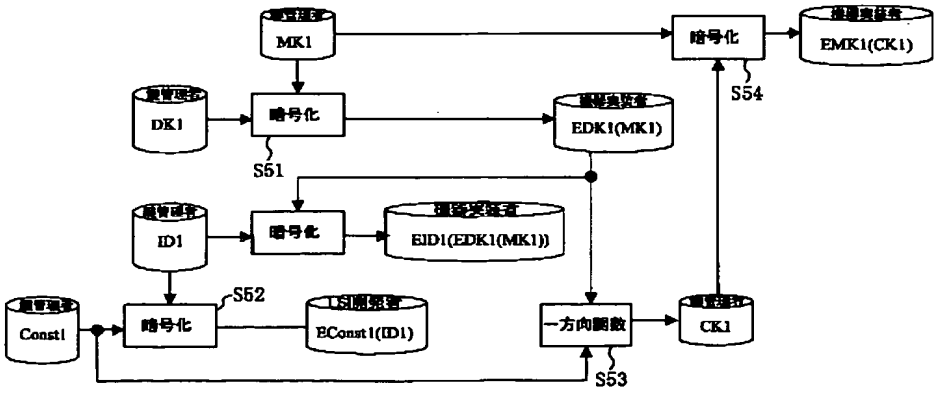
【図5】


tstMK1
暗号化
EtstMK1
(tstKEY1)
S22
tstDK1
暗号化
EtstDK1
(tstMK1)
S21
tstKEY1
暗号化
EtstKEY1
(EtstDK1(tstMK1))
S23
暗号化
EtstDK1
(EMK1(KEY1))
S24
S12
MK1
暗号化
EMK1
(KEY1)
DK1
暗号化
EDK1
(MK1)
S11
S13
KEY1
暗号化
EKEY1
(EDK1(MK1))

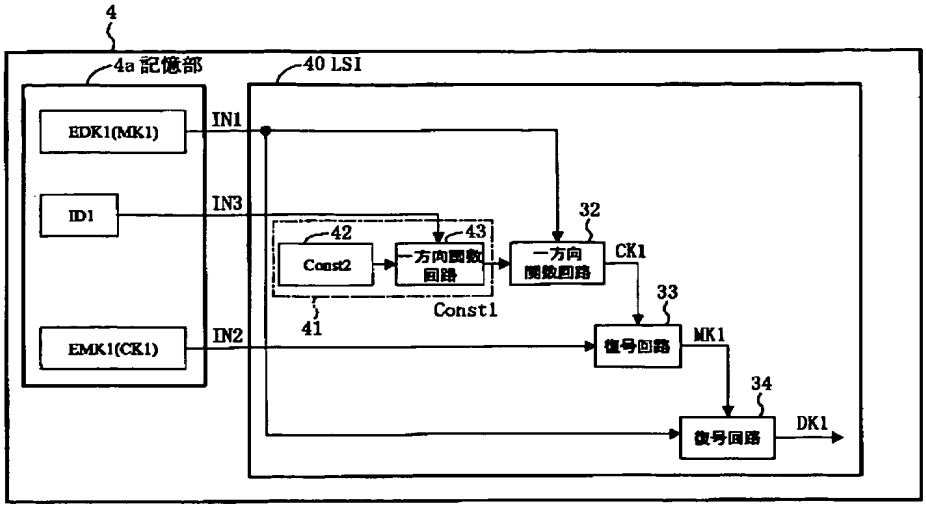
【図7】


S33
MK1
暗号化
EMK1(CK1)
DK1
暗号化
EDK1(MK1)
S31
Const1
一方向関数
CK1
S32
Const1

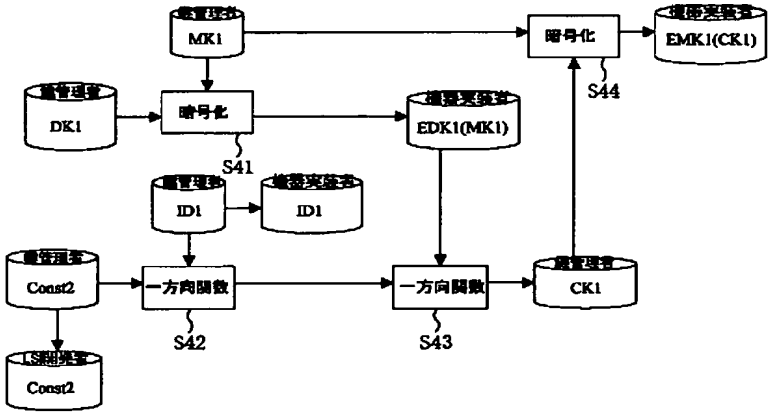
【図11】


MK1
暗号化
EMK1(CK1)
S54
DK1
暗号化
EDK1(MK1)
S51
ID1
暗号化
EID1(EDK1(MK1))
S52
Const1
暗号化
EConst1(ID1)
一方向関数
CK1
S53

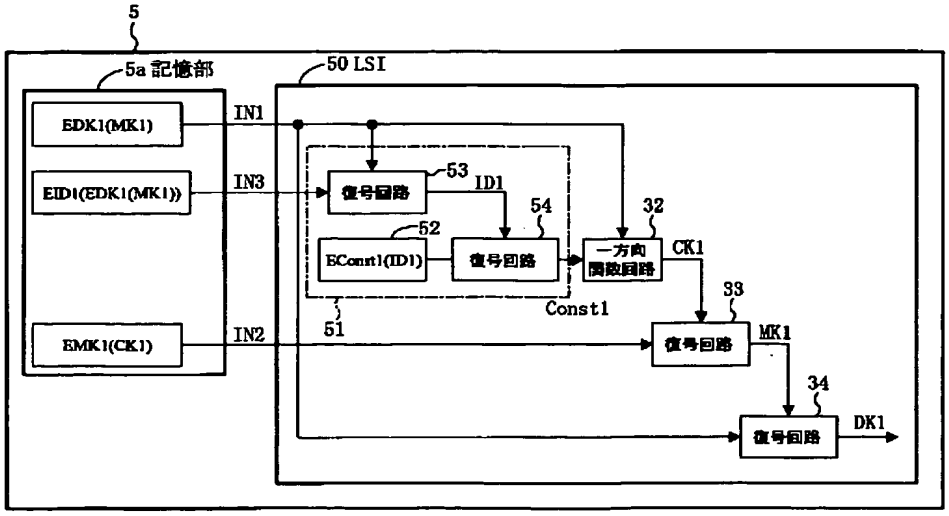
【図8】


4
4a 記憶部
40 LSI
EDK1(MK1)
IN1
ID1
IN3
42
43
Const2
一方向関数回路
Const1
41
32
CK1
一方向関数回路
33
EMK1(CK1)
IN2
復号回路
MK1
34
復号回路
DK1

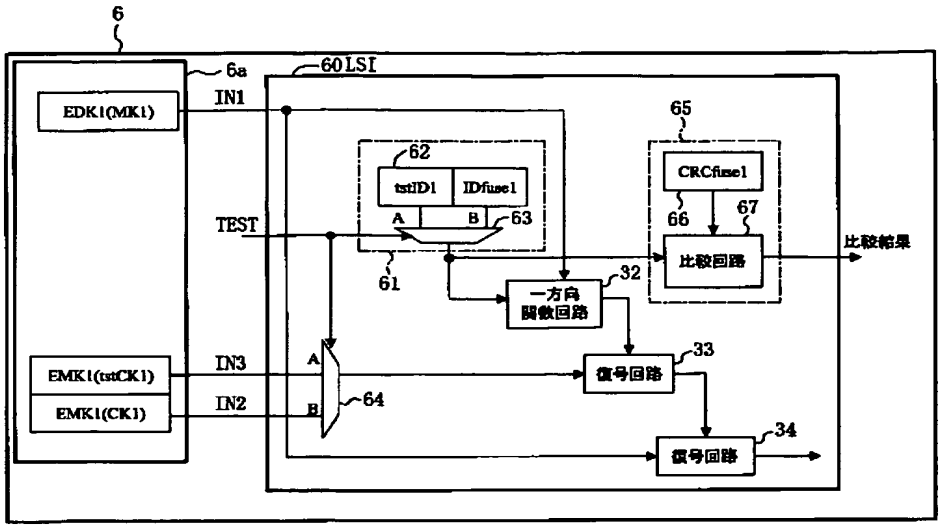
【図9】


MK1
暗号化
EMK1(CK1)
S44
DK1
暗号化
EDK1(MK1)
S41
ID1
ID1
Const2
一方向関数
一方向関数
CK1
S42
S43
Const2

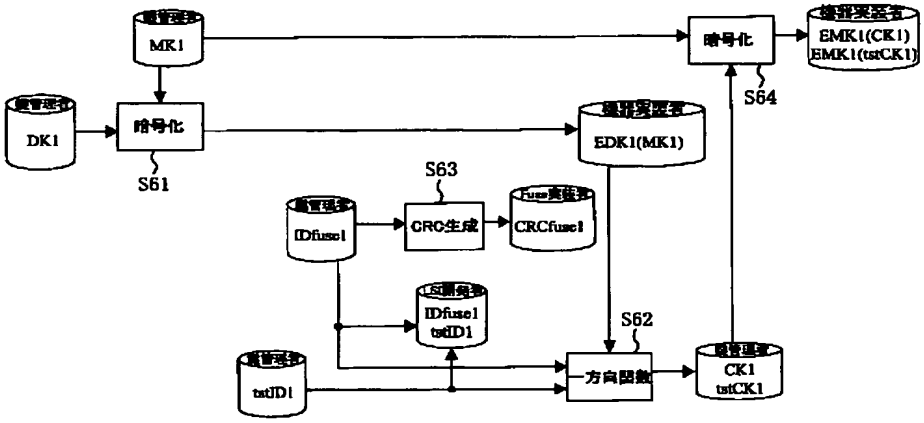
【図10】


5
5a 記憶部
50 LSI
EDK1(MK1)
IN1
EID1(EDK1(MK1))
IN3
復号回路
53
ID1
54
32
52
EConst1(ID1)
復号回路
一方向関数回路
CK1
Const1
51
33
EMK1(CK1)
IN2
復号回路
MK1
34
復号回路
DK1

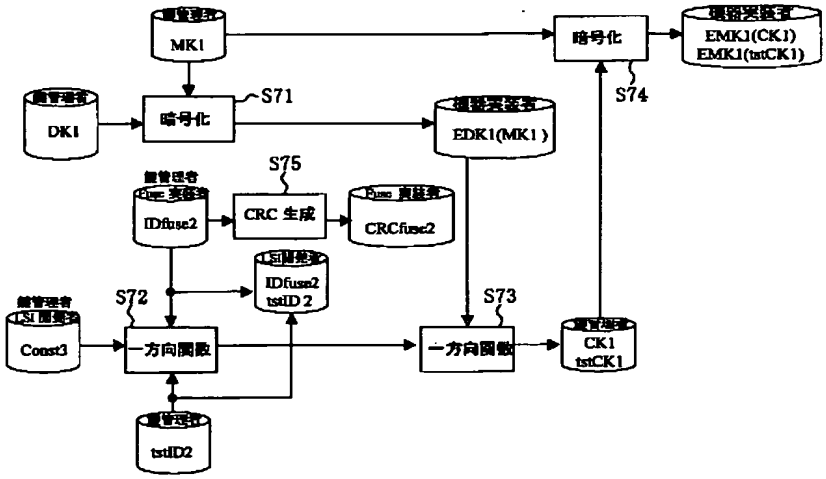
【図１２】


6
6a
60 LSI
EDK1(MK1)
IN1
62
tstID1
IDfuse1
A
B
63
65
CRCfuse1
66
67
TEST
比較結果
61
比較回路
32
一方向関数回路
EMK1(tstCK1)
IN3
A
33
復号回路
EMK1(CK1)
IN2
B
64
34
復号回路

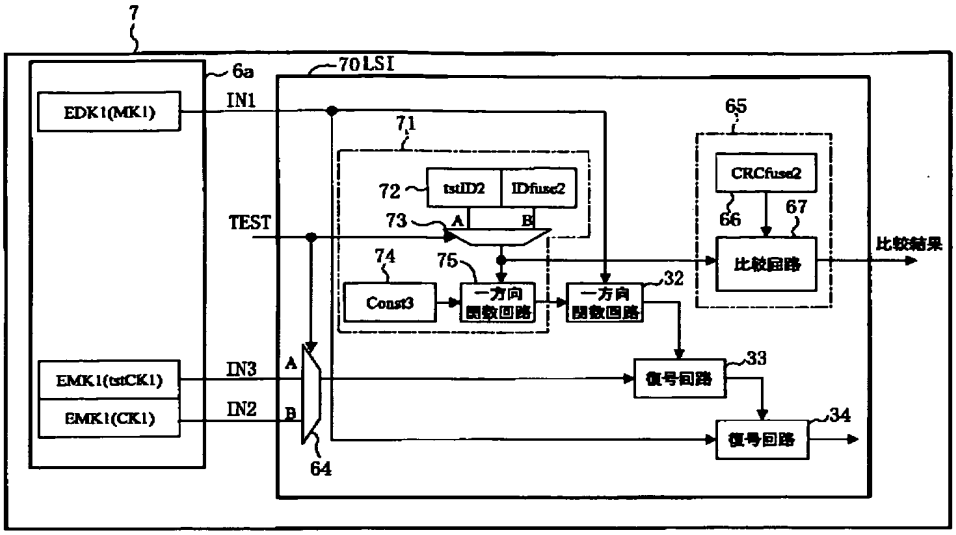
【図１３】


MK1
暗号化
EMK1(CK1)
EMK1(tstCK1)
S64
DK1
暗号化
EDK1(MK1)
S61
S63
IDfuse1
CRC生成
CRCfuse1
IDfuse1
tstID1
S62
tstID1
方向関数
CK1
tstCK1

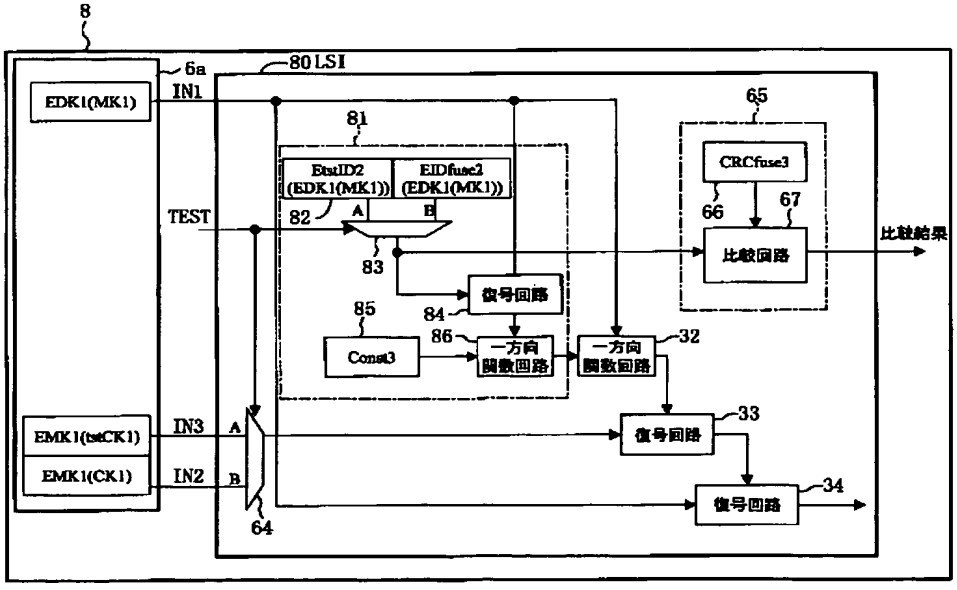
【図１５】


MK1
暗号化
EMK1(CK1)
EMK1(tstCK1)
S74
DK1
S71
暗号化
EDK1(MK1)
S75
IDfuse2
CRC 生成
CRCfuse2
IDfuse2
tstID2
S72
S73
Const3
方向関数
一方向関数
CK1
tstCK1
tstID2

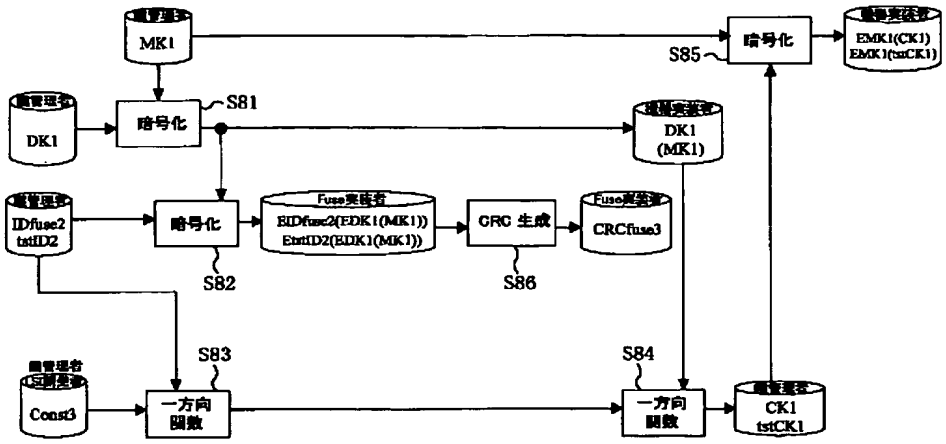
【図14】


7
6a
70LSI
EDK1(MK1)
IN1
71
65
72
tstID2
IDfuse2
CRCfuse2
TEST
73
A
B
66
67
比較結果
74
75
Const3
一方向関数回路
一方向関数回路
32
比較回路
EMK1(tstCK1)
IN3
A
33
復号回路
EMK1(CK1)
IN2
B
34
復号回路
64

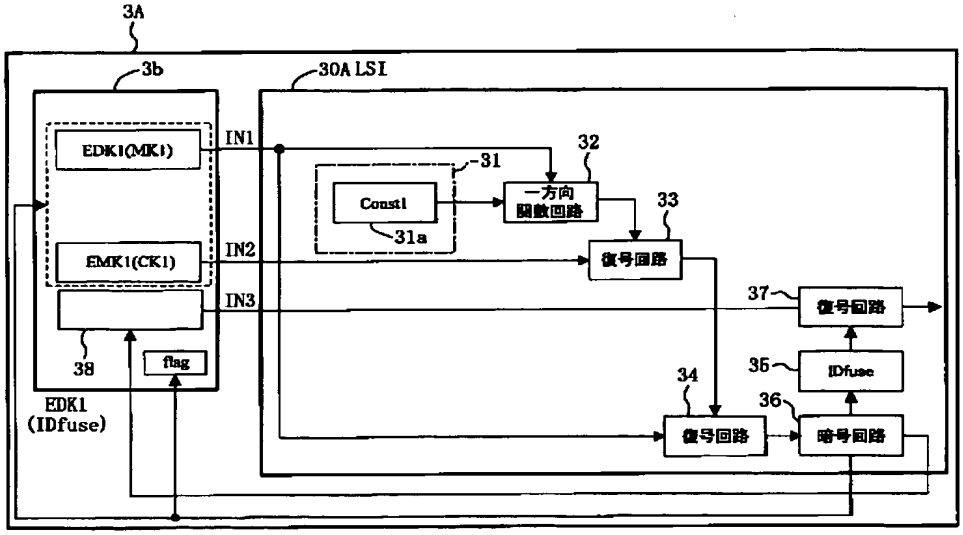
【図16】


8
6a
80LSI
EDK1(MK1)
IN1
81
65
EtstID2 (EDK1(MK1))
EIDfuse2 (EDK1(MK1))
CRCfuse3
TEST
82
A
B
66
67
比較結果
83
比較回路
復号回路
85
84
86
Const3
一方向関数回路
一方向関数回路
32
EMK1(tstCK1)
IN3
A
33
復号回路
EMK1(CK1)
IN2
B
34
復号回路
64

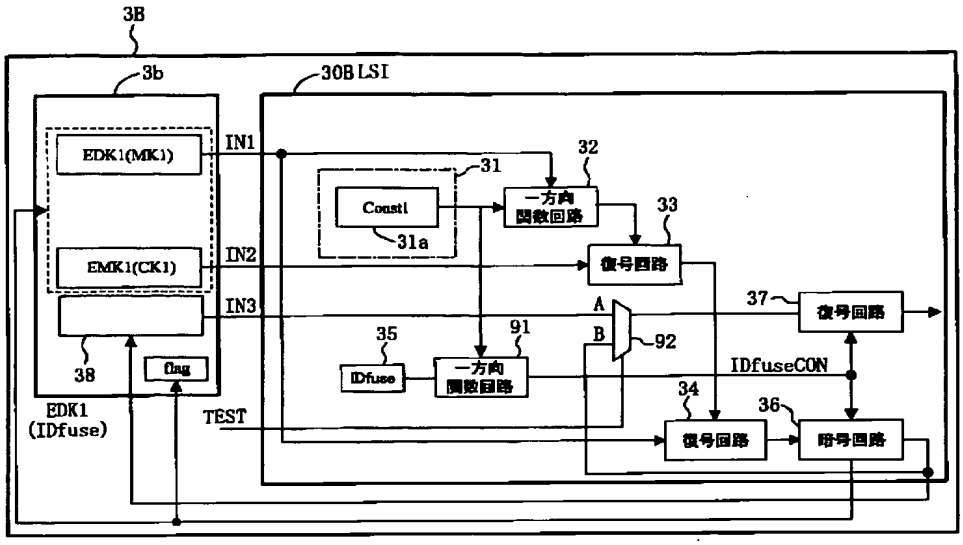
【図17】


MK1
暗号化
S85
EMK1(CK1)
EMK1(tstCK1)
DK1
暗号化
S81
DK1
(MK1)
IDfuse2
tstID2
暗号化
Fuse実装者
EIDfuse2(EDK1(MK1))
EtstID2(EDK1(MK1))
CRC 生成
CRCfuse3
S82
S86
S83
S84
Const3
一方向
関数
一方向
関数
CK1
tstCK1

【図18】


3A
3b
30A LSI
EDK1(MK1)
IN1
31
32
Const1
31a
一方向
関数回路
33
EMK1(CK1)
IN2
復号回路
37
復号回路
IN3
38
flag
35
IDfuse
34
36
EDK1
(IDfuse)
復号回路
暗号回路

【図19】



フロントページの続き

Fターム(参考) 5B017 AA03 BA07 CA05
5J104 AA16 EA07 NA02 NA35 NA37
NA42